Mathematics

OCT 9

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

Helmut Hasse

Band 177

Heft 4

Ausgegeben am 30. August 1937

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlagsbuchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.

Berlin W 35 und Leipzig

1937

Band 177. Heft 4.

Inhaltsverzeichnis.

	Seite
Hasse, Helmut, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. (Nach einer brieflichen Mitteilung von F. K. Schmidt in Jena.)	215
Zusatz bei der Korrektur. Von F. K. Schmidt in Jena	223
Lutz, Elisabeth, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques	238
Sz. Nagy, Julius v., Über Raumkurven vom Maximalindex	197
Rohrbach, Hans, Beweis einer zahlentheoretischen Ungleichung	193
Schulz, Werner, Über die Galoissche Gruppe der Hermiteschen Polynome	248

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgendeinem Grunde Textänderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von allen Abhandlungen 75 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion unter der Adresse:
An die Redaktion des Journals für die reine und angewandte Mathematik
Professor Dr. Helmut Hasse, Göttingen, Mathematisches Institut, Bunsenstr. 3-5.

Druck von Walter de Gruyter & Co., Berlin W 35
Printed in Germany

Beweis einer zahlentheoretischen Ungleichung.

Von *Hans Rohrbach* in Göttingen.

---

1. Es seien $m_1, m_2, \ldots, m_n$ natürliche Zahlen, $\{m_\varkappa, m_\lambda, \ldots, m_\varrho\}$ das kleinste gemeinschaftliche Vielfache von $m_\varkappa, m_\lambda, \ldots, m_\varrho$. Man bilde die beiden Summen

$$(1)\quad S_n = 1 - \sum_{\varkappa} \frac{1}{m_\varkappa} + \sum_{\varkappa<\lambda} \frac{1}{m_\varkappa m_\lambda} - \sum_{\varkappa<\lambda<\mu} \frac{1}{m_\varkappa m_\lambda m_\mu} + - \cdots + \frac{(-1)^n}{m_1 m_2 \cdots m_n} = \prod_{\nu=1}^{n} \left(1 - \frac{1}{m_\nu}\right)$$

und

$$(2)\quad T_n = 1 - \sum_{\varkappa} \frac{1}{m_\varkappa} + \sum_{\varkappa<\lambda} \frac{1}{\{m_\varkappa, m_\lambda\}} - \sum_{\varkappa<\lambda<\mu} \frac{1}{\{m_\varkappa, m_\lambda, m_\mu\}} + - \cdots + \frac{(-1)^n}{\{m_1, m_2, \ldots, m_n\}}.$$

Herr Hasse hat nun vermutet, *daß für jedes natürliche n die Ungleichung*

$$(3)\qquad S_n \leqq T_n$$

gilt. Im folgenden soll die Richtigkeit dieser Vermutung gezeigt werden.

Zu dem Zweck forme ich die Behauptung um, indem ich S_n und T_n mit $P_n = m_1 m_2 \cdots m_n$ multipliziere [1]). Dann ist

$$(4)\qquad \begin{aligned} P_n S_n &= m_1 m_2 \cdots m_n \prod_{\nu=1}^{n} \left(1 - \frac{1}{m_\nu}\right), \\ P_n T_n &= A(m_1, m_2, \ldots, m_n), \end{aligned}$$

wo $A(m_1, m_2, \ldots, m_n)$ die Anzahl der natürlichen Zahlen unterhalb $m_1 m_2 \cdots m_n$ bezeichnet, die weder durch m_1, noch durch $m_2, \ldots,$ noch durch m_n teilbar sind [2]). Sind nun speziell $m_\nu = p_\nu$ $(\nu = 1, 2, \ldots, n)$ voneinander verschiedene Primzahlen, so wird die Anzahl der durch keine dieser Primzahlen teilbaren natürlichen Zahlen unterhalb $p_1 p_2 \cdots p_n$ gegeben durch

$$A(p_1, p_2, \ldots, p_n) = p_1 p_2 \cdots p_n \prod_{\nu=1}^{n} \left(1 - \frac{1}{p_\nu}\right).$$

Allgemeiner beweist Dirichlet in seiner Zahlentheorie [3]), daß diese Formel auch dann noch gilt, wenn an Stelle der Primzahlen nur paarweise teilerfremde natürliche Zahlen gesetzt werden. Die hier betrachtete Ungleichung (3) liefert jetzt eine Verallgemeinerung dieser Dirichletschen Aussage; nach (3) und (4) gilt nämlich für *beliebige* natürliche Zahlen m_ν

$$(5)\qquad A(m_1, m_2, \ldots, m_n) \geqq m_1 m_2 \cdots m_n \prod_{\nu=1}^{n} \left(1 - \frac{1}{m_\nu}\right).$$

---

[1]) Statt mit P_n kann man auch mit einem beliebigen Vielfachen von P_n multiplizieren.

[2]) Das folgt z. B. sofort aus Pólya-Szegö, Aufgaben und Lehrsätze aus der Analysis **2**, Berlin 1925, Abschnitt VIII, S. 119, Aufg. 21.

[3]) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie (1894), § 11.

Genauer ergibt sich noch, daß das Gleichheitszeichen nur in dem Dirichletschen Fall paarweise teilerfremder Zahlen m_ν steht.

2. Zum Beweis brauche ich folgenden

Hilfssatz. Es sei T_n durch (2) *definiert und $P_n = m_1 m_2 \cdots m_n$. Ist dann t ein beliebiger (positiver) Teiler von P_n und r die Anzahl der natürlichen Zahlen unterhalb P_n, die durch t, aber durch keine der Zahlen m_ν teilbar sind, so ist*

$$0 \leqq r \leqq \frac{1}{t} P_n T_n. \tag{6}$$

Beweis. Ist $t \mid P_n$ derart, daß für ein ν zugleich $m_\nu \mid t$ ist, so ist $r = 0$. Es sei also $r > 0$, und $b_1, b_2, \ldots, b_r$ seien die Zahlen unterhalb P_n, die durch t, aber durch keins der m_ν teilbar sind. Man setze

$$\frac{m_\nu}{(t, m_\nu)} = k_\nu \qquad (\nu = 1, 2, \ldots, n). \tag{7}$$

Die Multipla von t unterhalb P_n sind

$$t, 2t, \ldots, \frac{P_n}{t} \cdot t.$$

Von diesen kommen unter den b_ϱ diejenigen Multipla *nicht* vor, die durch mindestens eine der Zahlen m_ν teilbar sind. Nun ist dann und nur dann ein Vielfaches ct durch ein m_ν teilbar, wenn

$$\frac{ct}{m_\nu} = \frac{ct}{k_\nu (t, m_\nu)} = \text{ganze Zahl},$$

also, wegen

$$\left(\frac{t}{(t, m_\nu)}, k_\nu\right) = \left(\frac{t}{(t, m_\nu)}, \frac{m_\nu}{(t, m_\nu)}\right) = 1,$$

wenn

$$c \equiv 0 \pmod{k_\nu}$$

ist. Daher ist die abzuschätzende Anzahl r gleich der Anzahl der natürlichen Zahlen unterhalb $\frac{P_n}{t}$, die durch keins der k_ν teilbar sind. Diese Anzahl wird durch

$$r = \frac{P_n}{t}\left[1 - \sum_\nu \frac{1}{k_\nu} + \sum_{\nu<\mu} \frac{1}{\{k_\nu, k_\mu\}} - + \cdots + \frac{(-1)^n}{\{k_1, k_2, \ldots, k_n\}}\right]$$

gegeben[4]). Mithin ist tr die Anzahl der natürlichen Zahlen unterhalb P_n, die durch keins der k_ν teilbar sind. Diese Anzahl ist aber, da nach (7) $k_\nu \mid m_\nu$ ist, höchstens gleich der Anzahl der natürlichen Zahlen unterhalb P_n, die durch keins der m_ν teilbar sind. Daher ist wegen der unter (4) angegebenen Bedeutung von $P_n T_n$

$$tr \leqq P_n T_n \tag{8}$$

und folglich der Hilfssatz bewiesen.

Für $n = 1$ ist $P_1 T_1 = m_1 - 1$ und

$$r = \frac{m_1}{t} - 1 \leqq \frac{m_1 - 1}{t}.$$

Hier steht das Gleichheitszeichen nur für $t = 1$. Dagegen kann, falls $n > 1$ ist, das Gleichheitszeichen in der rechten der Ungleichungen (6) auch für $t > 1$ auftreten. Ist z. B. m_1 das kleinste der m_ν und sind sämtliche m_ν Vielfache von m_1, ist ferner etwa

[4]) Vgl. Anm. 2.

$m_2 = qm_1$ mit $q > 1$ und $(q, m_1) = 1$, so wähle man $t = q$. Dann sind auch sämtliche k_ν Vielfache von m_1 und daher die Anzahlen der natürlichen Zahlen unterhalb $\frac{P_n}{t}$, die durch keins der k_ν bzw. keins der m_ν teilbar sind, einander gleich. In (8) steht also das Gleichheitszeichen.

3. *Beweis der Ungleichung* (3). Man multipliziere beide Seiten der Ungleichung (3) mit P_n und setze

$$Q_n = P_n S_n = (m_1 - 1)(m_2 - 1) \cdots (m_n - 1)$$

und

$$R_n = P_n T_n .$$

Dann lautet die Behauptung:

$$Q_n \leqq R_n .$$

Für $n = 1$ ist dies richtig, denn es ist $S_1 = T_1$, also auch $Q_1 = R_1$. Man nehme daher an, die Behauptung sei für alle natürlichen Zahlen bis $n - 1$ bewiesen. Dann liegen also unterhalb P_{n-1} genau R_{n-1} natürliche Zahlen, die durch keine der Zahlen $m_1, m_2, \ldots, m_{n-1}$ teilbar sind, und es ist $R_{n-1} \geqq Q_{n-1}$. Die R_{n-1} eben charakterisierten Zahlen seien $a_1, a_2, \ldots, a_{R_{n-1}}$. Ferner sei $(P_{n-1}, m_n) = d$.

Zur Bestimmung von R_n hat man nun abzuzählen, wieviele Zahlen x unterhalb P_n existieren, für die einerseits

$$(9) \qquad x \equiv a_1 \text{ oder } \equiv a_2 \cdots \text{ oder } \equiv a_{R_{n-1}} \pmod{P_{n-1}}$$

und andererseits

$$(10) \qquad x \equiv 1 \text{ oder } \equiv 2 \cdots \text{ oder } \equiv m_n - 1 \pmod{m_n}$$

ist. Wenn für eine Kombination einer Kongruenz (9) mit einer Kongruenz (10) eine Lösung vorhanden ist, so ist diese nur mod des kleinsten gemeinsamen Vielfachen von P_{n-1} und m_n bestimmt; aus einer Lösung folgen daher sofort d Lösungen des Kongruenzenpaares unterhalb $P_{n-1}m_n = P_n$. Ferner ist die notwendige und hinreichende Bedingung dafür, daß eine simultane Lösung des Kongruenzenpaares existiert, bekanntlich die, daß die Differenz der beiden auf der rechten Seite der Kongruenzen stehenden Glieder durch d teilbar ist. Um daher festzustellen, wieviele Kombinationen der festen Kongruenz

$$x \equiv a_\varrho \pmod{P_{n-1}}$$

mit einer der Kongruenzen (9) Lösungen liefern, muß man die Anzahl der zu $a_\varrho \bmod d$ kongruenten unter den Zahlen $1, 2, \ldots, m_n - 1$ bestimmen. Diese Anzahl ist aber

$$\frac{m_n}{d} - 1 \text{ bzw. } \frac{m_n}{d},$$

je nachdem a_ϱ durch d teilbar ist oder nicht. Nach dem Hilfssatz, angewandt für $n - 1$ statt n, ist nun, da d ein Teiler von P_{n-1} ist, die Anzahl der durch d teilbaren unter den R_{n-1} Zahlen a_ϱ höchstens gleich

$$\frac{1}{d} P_{n-1} T_{n-1} = \frac{1}{d} R_{n-1} .$$

Daher folgt: Mindestens $R_{n-1} - \frac{R_{n-1}}{d}$ der Zahlen a_ϱ liefern $\frac{m_n}{d}$ Kongruenzenpaare (9), (10), für die Lösungen vorhanden sind, während die übrigen a_ϱ je ein solches Kongruenzenpaar weniger liefern. Die Anzahl der Kongruenzenpaare, die Lösungen be-

sitzen, ist also mindestens

$$\left(R_{n-1} - \frac{R_{n-1}}{d}\right)\frac{m_n}{d} + \frac{R_{n-1}}{d}\left(\frac{m_n}{d} - 1\right) = \frac{R_{n-1}}{d}(m_n - 1).$$

Die Gesamtzahl der Lösungen, d. h. R_n, ist d-mal so groß, folglich ist

$$R_n \geqq R_{n-1}(m_n - 1), \tag{11}$$

womit auf Grund der Induktionsvoraussetzung die Behauptung bewiesen ist.

Daß das Gleichheitszeichen in der Ungleichung (3) und daher auch in (5) nur in dem Dirichletschen Fall paarweise teilerfremder Zahlen m_ν steht, ergibt sich folgendermaßen: Es seien $m_1, m_2, \ldots, m_n$ nicht paarweise teilerfremd und etwa $(m_1, m_2) > 1$, was durch geeignete Numerierung stets erreicht werden kann. Dann ist bei dem ersten Schritt des Induktionsverfahrens von $n = 1$ auf $n = 2$ der Hilfssatz für $n = 1$ und einen Teiler $t > 1$ anzuwenden, also bereits $Q_2 < R_2$ und daher nach (11)

$$R_n \geqq R_2(m_3 - 1)\cdots(m_n - 1) > Q_2(m_3 - 1)\cdots(m_n - 1) = Q_n.$$

4. *Bemerkung.* Läßt man die $m_\varkappa$ eine *unendliche* Folge natürlicher Zahlen

$$m_1, m_2, \ldots, m_n, \ldots \tag{12}$$

durchlaufen, so entstehen aus S_n bzw. T_n die unendlichen Reihen

$$1 - \sum_{\varkappa}\frac{1}{m_\varkappa} + \sum_{\varkappa<\lambda}\frac{1}{m_\varkappa m_\lambda} - \cdots \pm \sum_{\varkappa<\lambda<\cdots<\varrho}\frac{1}{m_\varkappa m_\lambda \cdots m_\varrho} \mp \cdots \tag{13}$$

bzw.

$$1 - \sum_{\varkappa}\frac{1}{m_\varkappa} + \sum_{\varkappa<\lambda}\frac{1}{\{m_\varkappa m_\lambda\}} - \cdots \pm \sum_{\varkappa<\lambda<\cdots<\varrho}\frac{1}{\{m_\varkappa, m_\lambda, \ldots, m_\varrho\}} \mp \cdots. \tag{14}$$

Wenn nun die Folge (12) die Eigenschaft hat, daß die Reihe (14) und folglich auch die Reihe (13) absolut konvergent ist, so sind S_n bzw. T_n bei geeigneter Anordnung der Reihenglieder Partialsummen der Reihe (13) bzw. (14), und es gilt, falls S bzw. T die Summen dieser Reihen bedeuten, nach (3)

$$S \leqq T.$$

Eingegangen 28. September 1936.

Über Raumkurven vom Maximalindex[1]).

Von *Julius* (*Gyula*) *v. Sz. Nagy* in Szeged (Ungarn).

1. Einleitung.

Unter einer einzügigen ebenen Kurve verstehen wir im folgenden eine Elementarkurve im Sinne von C. Juel, d. h. ein reelles, eindeutiges, stetiges und mit stetiger Tangente versehenes Kreisbild in der projektiven Ebene, welches aus endlich vielen Konvexbogen besteht [2]). Eine einzügige Raumkurve bedeutet im folgenden ein reelles, eindeutiges, stetiges und mit stetiger Tangente und Schmiegebene versehenes Kreisbild im dreidimensionalen projektiven Raum, welches aus endlich vielen Bogen dritter Ordnung besteht. Eine ebene Kurve bzw. eine Raumkurve kann aus mehreren Zügen bestehen, dann sind ihre Züge einzügige ebene bzw. Raumkurven. (Wir werden im folgenden mit C bzw. N eine ebene Kurve bzw. einen ihrer Züge, mit G bzw. M eine Raumkurve bzw. einen ihrer Züge bezeichnen.)

Die Ordnung bzw. der Index einer Raumkurve ist die Maximal- bzw. Minimalanzahl der Punkte (jeden Punkt mit seiner Vielfachheit gerechnet), in denen die Kurve von einer Ebene getroffen wird. Eine Raumkurve n-ter Ordnung ist vom Maximalindex, wenn sie den Index $n - 2$ hat.

In der Literatur haben drei Verfasser allgemeine Untersuchungen über die Raumkurven vom Maximalindex veröffentlicht, nämlich C. Juel, H. Mohrmann und Julius (Gyula) v. Sz. Nagy [3]).

Anschließend an ihre Resultate und unsere Untersuchungen [4]) über die ebenen Kurven vom Maximalklassenindex und die Flächen vom Maximalindex werden wir die

---

[1]) Diese Arbeit ist eine in mehreren Punkten veränderte Umarbeitung einer ungarischen Abhandlung des Verfassers, Math. u. Naturwiss. Anzeiger d. Ungarischen Akademie der Wiss. **54** (1936), 685—711.

[2]) O. Haupt hat in der Arbeit: Zur Juelschen Theorie der reellen, ebenen Kurven 4. Ordnung (Sitz.-Ber. d. bayer. Akad. d. Wiss., Math. Phys. Klasse 1925, 1—8, insb. 6—7) bewiesen, daß *jede* ebene Kurve von beschränkter Ordnung und vom Maximalindex aus endlich vielen Konvexbogen besteht.

[3]) C. Juel, Die gewundenen Kurven vom Maximalindex auf einer Regelfläche zweiter Ordnung, Kgl. Danske Selsk. Skr., Naturv. og. Math. Afd., (8) **2** (1917) Nr. 5, 279—294.

H. Mohrmann, 1. Über algebraische und nichtalgebraische gewundene Kurven n-ter Ordnung vom Maximalindex, Math. Annalen **78** (1917), 171—176.

2. Gewundene reelle Kurvenzüge beliebig hoher Ordnung ohne reelle Singularität, Sitz.-Ber. d. bayer. Akad. d. Wiss., Math. Phys. Klasse 1916, 201—208.

3. Gewundene Kurven vom Maximalindex, Gött. Nachr. 1916, 197—198.

Julius v. Sz. Nagy, 1. Über die reellen Züge algebraischer ebener und Raumkurven, Math. Annalen **77** (1916), 416—429.

Diese Arbeiten werden im folgenden mit J, M 1, M 2, M 3 bzw. N 1 zitiert.

[4]) Julius v. Sz. Nagy, 2. Über Kurven von Maximal-Klassenindex. Über Kurven von Maximalindex, Math. Annalen **89** (1923), 32—75; **90** (1924), 150—151.

wichtigsten Eigenschaften der Raumkurven vom Maximalindex untersuchen. Unsere Resultate beziehen sich auf Reduzibilität oder Irreduzibilität, auf das Geschlecht und andere charakteristische Zahlen der Raumkurven vom Maximalindex.

Unsere Untersuchungen berühren sich mit einer von O. Haupt herrührenden Verallgemeinerung der Ordnung einer ebenen Kurve[5]). Die Ordnung bzw. der Index einer ebenen Kurve C in bezug auf ein ebenes Kurvensystem ist die Maximal- bzw. Minimalanzahl der Punkte, in denen die Kurve von den Kurven des Systems — außer den in die Grundpunkte des Systems allgemein fallenden Punkten — getroffen werden kann. Ist dieses Kurvensystem linear, algebraisch und dreidimensional in bezug auf C, und hat die Kurve C in jedem Punkte eine mit dem Punkte sich stetig ändernde Krümmung, so kann man der Kurve C eine Raumkurve G zuordnen, die von einer Ebene in so vielen Punkten getroffen wird wie C von der entsprechenden Kurve des Systems außerhalb der Grundpunkte.

Auf diese Weise werden wir die Existenz reduzibler Raumkurven vom Maximalindex beweisen und solche Raumkurven darstellen[6]).

2. Zusammenfassung der bisher bekannten allgemeinen Sätze über die Raumkurven vom Maximalindex.

Wir halten es für nützlich, sogar für nötig, die bisher bekannten Sätze zusammenzufassen.

1. G sei eine Raumkurve vom Maximalindex; bewegt sich ein Punkt P im Raume, ohne jemals in G zu fallen, so ändert sich die Anzahl der durch P an G gehenden Schmiegebenen und Doppelsekanten dann und nur dann, wenn P die Tangentenfläche von G überschreitet. Die Änderung ist für die Anzahl der Doppelsekanten bzw. der Schmiegebenen $+1$ oder -1 bzw. -2 oder $+2$[7]).

---

3. Über die charakteristischen Zahlen einer Kurve vom Maximalklassenindex, Math. Annalen **100** (1928), 164—178.

4. Über die reellen Züge der ebenen Kurven vom Maximalklassenindex, Math. Annalen **100** (1928), 179—187.

5. Über die reduziblen ebenen Kurven gegebener Klasse vom Maximalklassenindex mit der Maximalanzahl ineinander liegender Ovale, Math. Annalen **103** (1930), 502—515.

6. Über die irreduziblen ebenen Kurven von Maximalindex, Acta Math. Szeged **3** (1927), 96—106.

7. Über die ebenen Kurven von Maximalindex und von Maximalklassenindex, Jahresbericht d. DMV. **41** (1931), 82—87.

8. Einige Sätze über ebene Elementarkurven, Acta Math. Szeged **5** (1931), 83—89.

9. Über die Ordnung der ebenen Kurven von Maximalklassenindex, Math. Zeitschrift **35** (1932), 80—92.

10. Über die Ungleichungen für die Ordnung der ebenen Kurven vom Maximalklassenindex, Math. Zeitschrift **37** (1933), 493—513.

11. Über Flächen vom Maximalindex, Math. Annalen **98** (1927), 657—683.

12. Untersuchungen über die Flächen vom Maximalindex (Ungarisch), Math. u. Naturwiss. Anzeiger d. Ung. Akademie d. Wiss. **53** (1935), 420—474.

Diese Arbeiten werden im folgenden mit N 2, N 3, . . . , N 12 zitiert.

[5]) O. Haupt, Zur Theorie der Ordnung reeller Kurven in der Ebene bezüglich vorgegebener Kurvenscharen, Monatshefte f. Math. u. Phys. **40** (1933), 1—53. Der Begriff des Index wurde von O. Haupt in der Arbeit: Über ebene Bogen und Kurven vom Maximalindex im weiteren Sinne, Sitzungsber. d. bayer. Akad. d. Wiss. 1935, 37—70, erweitert. Nach dieser Definition bedeutet die Ordnung bzw. der Index einer ebenen Kurve die Maximal- bzw. Minimalanzahl der Schnittpunkte, in denen die Kurve von ihren *Sekanten* getroffen werden kann. Diese Definition läßt sich auch auf die Raumkurven übertragen. Wir gehen aber darauf nicht näher ein.

[6]) Wir bemerken, daß die vor einiger Zeit erschienene Arbeit von P. Scherk, Über reelle geschlossene Raumkurven vierter Ordnung, Math. Annalen **112** (1936), 743—766, die Raumkurven vierter Ordnung auch vom Gesichtspunkte des Index aus untersucht. — Verf. dankt Herrn P. Scherk für einige Bemerkungen bezüglich der vorliegenden Arbeit.

[7]) J, 280—281. · Dieser Satz sowie die Sätze 3 und 5 wurden von C. Juel nur für einzügige Raumkurven ausgesprochen. Sein Beweis gilt aber offenbar auch für mehrzügige Raumkurven vom Maximalindex.

2. Die Züge der Raumkurven vom Maximalindex sind alle vom Maximalindex. Die Raumkurven vom Maximalindex haben keinen Zug und keine Schleife vom Index Null [8]).

3. Die Raumkurven vom Maximalindex haben weder doppeltberührende noch hyperoskulierende Ebenen [9]).

4. Jede zentrale Projektion einer Raumkurve vom Maximalindex ist eine ebene Kurve vom Maximalindex.

5. Eine Raumkurve n-ter Ordnung vom Maximalindex wird von jeder Ebene, die durch eine Tangente der Kurve hindurchgeht, in n Punkten getroffen (jeden Punkt mit seiner Vielfachheit gerechnet) [10]).

6. Eine Raumkurve n-ter Ordnung vom Maximalindex hat höchstens $n-2$ Züge. Erreicht die Anzahl der Züge dieses Maximum, so sind alle Züge von dritter Ordnung. Die Raumkurve hat in diesem Fall keine Singularität, und ihre Projektion aus einem (außerhalb der Kurve liegenden) Punkt hat entweder $h = \binom{n-2}{2}$ oder $h-1$ Doppelpunkte [11]).

7. Genügen die positiven ganzen Zahlen $n, k, i_1, i_2, \ldots, i_k$ der Gleichung

$$i_1 + i_2 + \cdots + i_k = n - 2,$$

so gibt es Raumkurven n-ter Ordnung vom Maximalindex, die aus k Zügen von den Indizes $i_1, i_2, \ldots, i_k$ bestehen [12]).

8. Die auf einer Regelfläche zweiter Ordnung liegenden einzügigen Raumkurven n-ter Ordnung vom Maximalindex zerfallen in zwei Arten [13]): Eine Raumkurve erster Art wird von den Erzeugenden des einen bzw. des anderen Systems in einem bzw. in $n-1$ verschiedenen Punkten geschnitten. Eine solche Raumkurve $(n-1;\ 1)$ hat keinen Doppelpunkt. Eine Raumkurve zweiter Art wird von den Erzeugenden des einen Systems in $n-2$ verschiedenen Punkten, von denen des anderen aber in zwei oder 0 Punkten getroffen. Eine solche Raumkurve $(n-2;\ 2, 0)$ hat $n-3$ Doppelpunkte.

9. Auf einer Regelfläche zweiter Ordnung gibt es immer einzügige Raumkurven n-ter Ordnung vom Maximalindex und vom Typus $(n-1; 1)$ oder $(n-2; 2, 0)$ und zwar von beiderlei Art [14]).

10. Ist G eine auf einer Regelfläche zweiter Ordnung liegende einzügige Raumkurve n-ter Ordnung und vom Maximalindex, so ist die Gesamtzahl ihrer wirklichen und scheinbaren Doppelpunkte für einen (außerhalb der Kurve liegenden Punkt) entweder $\binom{n-1}{2}$ oder $\binom{n-1}{2} - 1$ [15]).

---

[8]) M 1, 172; N 1, 417.

[9]) J, 282; M 1, 172.

[10]) J, 282.

[11]) M 1, 172—173. Der Beweis von H. Mohrmann gibt die Anzahl der scheinbaren Doppelpunkte nur für solche Punkte P des Raumes an, die auf einer Doppelsekante eines Zuges liegen. Für solche Punkte P ist diese Anzahl gleich h. Auf Grund des Satzes 1 kann man leicht einsehen, daß die Anzahl der scheinbaren Doppelpunkte in bezug auf solche P, durch welche keine Tangente und Doppelsekante eines Zuges hindurchgehen, gleich $h-1$ ist. Liegt der Punkt P auf einer Tangente der Raumkurve, so ist ein scheinbarer Doppelpunkt offenbar ein scheinbarer Rückkehrpunkt erster Art.

[12]) N 1, 429; M 1, 175.

[13]) J, 284—286; M 1, 176; M 2, 206—208.

[14]) J, 292.

[15]) J, 289; M 1, 175.

11. Ist G eine auf einer Regelfläche zweiter Ordnung liegende einzügige Raumkurve n-ter Ordnung und vom Maximalindex, so gehen entweder n oder $n-2$ Schmiegebenen durch einen beliebigen Punkt des Raumes an G. Eine Gerade des Raumes schneidet höchstens $2n-2$ Tangenten der Kurve G. Es gibt aber Geraden, von denen $0, 2, 4, \ldots, 2n-2$ Tangenten geschnitten werden [16]).

3. Reduzibilität und Irreduzibilität der Raumkurven vom Maximalindex.

Wir nennen eine mehrzügige Raumkurve *zerfallend* oder *reduzibel*, wenn ihre Züge in zwei oder mehrere Systeme so gruppiert werden können, daß die Summe der Ordnungen der Raumkurven, die von den Zügen je eines Systems gebildet werden, der Ordnung der Raumkurve gleich ist. Die Raumkurve G von n-ter Ordnung zerfällt also dann in die Raumkurven $G_1, G_2, \ldots, G_k$ von n_1-, n_2-, $\ldots$, n_k-ter Ordnung, wenn die Kurven $G_1, G_2, \ldots, G_k$ zusammen jeden Zug von G genau einmal enthalten und sonst keinen, und wenn $n = n_1 + n_2 + \cdots + n_k$ ist [17]). Die Kurven $G_1, G_2, \ldots, G_k$ werden auch Faktorkurven der Raumkurve G genannt.

Hat die Raumkurve G nur einen Zug oder zerfällt sie bei keiner Einteilung ihrer Züge, so ist sie *einfach* oder *irreduzibel*.

Auf ähnliche Weise wie für ebene Kurven und Flächen vom Maximalindex [18]) kann man auch für Raumkurven den folgenden Satz beweisen:

I. *Ist eine Raumkurve vom Maximalindex reduzibel, so sind ihre Faktorkurven wieder vom Maximalindex.*

Im entgegengesetzten Falle gäbe es nämlich eine Raumkurve G n-ter Ordnung vom Maximalindex, die in die Raumkurven $G_1, G_2, \ldots, G_k$ von n_1-, n_2-, $\ldots$, n_k-ter Ordnung zerfällt, von denen aber die Kurve G_1 den Index $i_1 \leqq n_1 - 4$ hat. Es gäbe dann eine Ebene, welche die Kurve G_1 in i_1, die Kurven $G_2, G_3, \ldots, G_k$ in höchstens $n_2, n_3, \ldots, n_k$, die Kurve G also in höchstens

$$i_1 + n_2 + n_3 + \cdots + n_k \leqq (n_1 + n_2 + \cdots + n_k) - 4 = n - 4$$

Punkten trifft. Die Raumkurve G n-ter Ordnung hätte also nicht den Maximalindex $n-2$.

Es gilt auch der folgende Satz [19]):

II. *Eine Raumkurve vom Maximalindex ist dann und nur dann irreduzibel, wenn ihr Index gleich der Summe der Indizes ihrer Züge ist. Ist die Ordnung der Raumkurve vom Maximalindex um $2k$ größer als die Summe der Indizes ihrer Züge, so zerfällt die Kurve in k irreduzible Faktorkurven. Die Zerlegung einer reduziblen Raumkurve vom Maximalindex in irreduzible Faktorkurven ist eindeutig.*

Zerfällt die Raumkurve G vom Maximalindex in die k ($k > 1$) irreduziblen Kurven $G_1, G_2, \ldots, G_k$ und bezeichnen $n, n_1, n_2, \ldots, n_k$ bzw. $i, i_1, i_2, \ldots, i_k$ die Ordnungen bzw. die Indizes der Kurven $G, G_1, G_2, \ldots, G_k$, so bestehen die Gleichungen

$$n = n_1 + n_2 + \cdots + n_k = i + 2, \quad n_1 = i_1 + 2, \quad n_2 = i_2 + 2, \ldots, n_k = i_k + 2.$$

Daraus folgt die Gleichung

$$n - 2 = i = i_1 + i_2 + \cdots + i_k + 2(k-1).$$

Der Index i_h der Raumkurve G_h ($h = 1, 2, \ldots, k$) ist mindestens gleich der Summe

---

[16]) J, 290 und 298.
[17]) M 1, 172; N 2, 62—68, 74—75; N 11, 680.
[18]) N 2, 63, 66—67; N 11, 680.
[19]) Vgl. N 2, 63, 66—67; N 11, 680.

der Indizes ihrer Züge. Daraus folgt die Ungleichung

$$n - 2 = i \geqq i'_1 + i'_2 + \cdots + i'_s + 2(k-1) > i'_1 + i'_2 + \cdots + i'_s,$$

wo $i'_1, i'_2, \ldots, i'_s$ die Indizes der Züge von G bedeuten.

Aus der letzten Ungleichung folgt, daß der Index einer reduziblen Raumkurve vom Maximalindex immer größer ist als die Summe der Indizes ihrer Züge und daß eine Raumkurve vom Maximalindex, deren Index gleich der Summe der Indizes ihrer Züge ist, irreduzibel ist.

Wir projizieren die Raumkurve G von einem (außerhalb von G liegenden) Punkte S aus auf eine Ebene σ. Die Ordnung und der Index der so erhaltenen ebenen Kurve C sind offenbar gleich der Ordnung und dem Index von G. Ebenso hat ein Zug von G dieselbe Ordnung und denselben Index wie seine ebene Projektion.

Ist also die Ordnung von G um $2k$ $(k > 1)$ größer als die Summe der Indizes ihrer Züge, so gilt dies auch für die ebene Kurve C. Dann zerfällt aber die ebene Kurve C vom Maximalindex in k irreduzible Faktorkurven [20]). Wir bezeichnen sie mit $C_1, C_2, \ldots, C_k$, ihre Ordnungen mit $n_1, n_2, \ldots, n_k$.

Ist G_h die Teilkurve von G, deren ebene Projektion die Kurve C_h ist, so wird G_h von einer durch den Punkt S hindurchgehenden Ebene entweder in n_h oder in $n_h - 2$ Punkten geschnitten. Da die Kurve C_h irreduzibel ist, ist ihr Index gleich der Summe der Indizes ihrer Züge. Dasselbe gilt auch für die Kurve G_h, weil sie höchstens den Index $n_h - 2$ hat und weil jeder Zug von G_h denselben Index hat wie seine ebene Projektion. Die Kurve G_h wird also von jeder Ebene in mindestens $n_h - 2$ Punkten getroffen. Sie wird aber von keiner Ebene in mehr als n_h Punkten getroffen.

Um dies zu beweisen, genügt es wegen Satz 5 zu zeigen, daß die Kurve G_h von jeder Ebene, die durch eine beliebige ihrer Tangenten hindurchgeht, in n_h Punkten getroffen wird.

Nach Satz 5 wird die Raumkurve G von jeder Ebene π durch eine Tangente p von G_h in n Punkten getroffen. Dreht man nun die Ebene π um die Achse p, so bleibt also die Anzahl der gemeinsamen Punkte der Ebene mit G und wegen Satz 3 auch mit G_h ungeändert. Die Ebene (S, p) trifft die Raumkurve G_h in ebensoviel Punkten wie die Schnittgerade der Ebenen (S, p) und π die ebene Kurve C_h vom Maximalindex. Diese Gerade berührt C_h, sie trifft C_h also in n_h Punkten. Daraus folgt, daß die Raumkurve G_h die Ordnung n_h hat und somit vom Maximalindex ist.

Damit haben wir bewiesen, daß die Kurve G in die irreduziblen Kurven $G_1, G_2, \ldots, G_k$ zerfällt.

Wäre die Zerlegung einer reduziblen Raumkurve vom Maximalindex in irreduzible Faktorkurven nicht eindeutig, so könnte man die ebene Kurve C vom Maximalindex auf mehrere Arten in irreduzible Faktorkurven zerlegen. Dies ist aber unmöglich. Die polare Figur der Kurve C in bezug auf einen Kreis ihrer Ebene ist eine ebene Kurve K n-ter Klasse vom Maximalklassenindex. Bilden die Punkte der Ebene, die $n - 2$ Tangenten an K senden, k zusammenhängende Gebiete $T_1, T_2, \ldots, T_k$, so zerfällt die Kurve K in k irreduzible Faktorkurven $K_1, K_2, \ldots, K_k$. Die Kurve K_h besteht aus den Zügen der Kurve K, von denen das Gebiet T_h begrenzt wird [21]). Aus der eindeutigen Zerlegung der Kurve K vom Maximalklassenindex folgt dieselbe auch für die Kurven C und G vom Maximalindex.

---

[20]) N 2, 66—67.

[21]) N 2, 65; N 4, 179.

Damit haben wir die Richtigkeit des Satzes II bewiesen.

Aus den beiden obigen Sätzen folgt der Satz:

III. *Eine k-zügige irreduzible Raumkurve vom Maximalindex bleibt auch dann irreduzibel und vom Maximalindex, wenn man h ihre Züge* $(h < k)$ *wegläßt.*

Für die Darstellung reduzibler Raumkurven vom Maximalindex benötigen wir einige Hilfssätze über algebraische ebene Kurven vom Maximalindex.

4. Hilfssätze über algebraische ebene Kurven vom Maximalindex.

Es gilt der folgende Satz:

Stellen die Gleichungen

$$e_h(x, y) \equiv y - a_h x = 0,\ f_k(x, y) \equiv y - b_k x = 0\ (h = 1, 2, \ldots, n-1; k = 1, 2, \ldots, n)$$

$2n - 1$ *voneinander verschiedene reelle Geraden dar, deren Reihenfolge in dem einen Drehsinne*

$$f_1, e_1, f_2, e_2, \ldots, f_{n-1}, e_{n-1}, f_n$$

ist, so stellt die Gleichung

$$e_1 e_2 \cdots e_{n-1} - f_1 f_2 \cdots f_n = 0$$

eine ebene algebraische Kurve K vom Maximalindex dar, deren Ordnung, Klasse bzw. Geschlecht auch hinsichtlich der Realität n, $2n - 2$ bzw. 0 ist. Ihr Klassenindex ist Null. Jeder Kegelschnitt durch den $(n - 1)$-fachen Punkt und einen Punkt eines bestimmten Bogens von K hat außer den in diese zwei Punkte fallenden n Punkten höchstens n und mindestens $n - 2$ Punkte mit K gemeinsam.

Die Kurve K hat im Ursprung 0 des Koordinatensystems einen gewöhnlichen $(n - 1)$-fachen Punkt mit den Tangenten $e_1, e_2, \ldots, e_{n-1}$. Jeder Strahl des durch 0 hindurchgehenden Strahlenbüschels hat außer den in 0 fallenden $n - 1$ Punkten einen und nur einen Punkt mit K gemeinsam.

Daraus folgt, daß alle $n - 1$ Tangenten des $(n - 1)$-fachen Punktes 0 einfach sind, daß keine andere Tangente von K durch 0 geht, und daß 0 der einzige singuläre Punkt von K ist.

Das algebraische und das Realitätsgeschlecht [22]) der Kurve K sind Null; denn ein $(n - 1)$-facher Punkt ist gleich $\frac{(n-1)(n-2)}{2}$ Doppelpunkten zu rechnen.

Die von 0 ausgehenden Halbgeraden der Geraden e_h und f_k lassen sich durch e_h' und e_h'' bzw. f_k' und f_k'' so bezeichnen, daß die Reihenfolge der einfachen (und im Innern keine dieser $4n - 2$ Halbgeraden enthaltenden) Winkelräume im angenommenen Drehsinne

$$(f_n', f_1'),\ (f_1', e_1'), \ldots, (e_{n-1}', f_n''),\ (f_n'', f_1'),\ (f_1'', e_1''), \ldots,\ (e_{n-1}'', f_1')$$

ist. Wir können annehmen, daß die positive y-Achse und damit auch der Punkt $A = (0, 1)$ von K in den Winkelraum (f_n', f_1') fällt.

Dreht man eine Gerade g von der y-Achse ausgehend im obigen Sinne um 0, so bewegt sich der n-te Schnittpunkt P der Geraden g mit K von A ausgehend monoton auf K. Der Punkt P gelangt nacheinander in die Winkelräume (f_n', f_1'), (f_1'', e_1''), (e_1', f_2'), (f_2'', e_2''), (e_2', f_3') usw., indem er den ersten, dritten usw. Winkelraum im uneigentlichen Punkt von f_1, f_2 usw., den zweiten, vierten usw. aber in 0 verläßt.

So sieht man leicht ein, daß die Kurve K die Gerade e_h $(h = 1, 2, \ldots, n - 1)$ auf derjenigen Seite von e_h berührt, welche zu A entgegengesetzt ist.

---

[22]) N 3, 164—165; N 4, 179.

Eine ebene Kurve n-ter Ordnung vom Maximalindex und vom Geschlecht p hat $w = n - 2 + 2p$ Wendetangenten [23]). Die Kurve K hat also $n - 2$ Wendetangenten. Keine von ihnen geht durch den Punkt 0. Daher gibt es auf der Strecke OA und auf der negativen y-Achse zwei Punkte B und C so, daß die Strecke BC von keiner Wendetangente von K getroffen wird. Die Strecke BC hat keinen Punkt außer 0 mit K gemeinsam.

Durchläuft nun ein Punkt Q von B aus die Strecke BC, so ändert sich die Anzahl der von ihm an die Kurve K gehenden Tangenten dann und nur dann, wenn er die Kurve in 0 überschreitet. Dort überschreitet er $n - 1$ konvexe Bogen von K, und zwar jeden von der konvexen Seite nach der konkaven. Daher sendet der Punkt B $2n - 2$ Tangenten mehr an K als C.

Nach der ersten Plückerschen Formel hat K die algebraische Klasse $2n - 2$. Somit ist auch die Realitätsklasse von K gleich $2n - 2$, und B bzw. C sendet $2n - 2$ bzw. keine Tangenten an K. Die Kurve K ist also vom Klassenindex Null.

Der in den Winkelräumen (e_1', f_2') und (f_2'', e_2'') liegende Pseudozug M_1 von K ist vom Index Eins, weil er mit der Geraden f_2 nur einen einfachen Schnittpunkt (den uneigentlichen Punkt von f_2) hat. Allgemein ist der in den Winkelräumen (e_k', f_{k+1}') und (f_{k+1}'', e_{k+1}'') liegende Pseudozug M_k vom Index Eins ($k = 1, 2, \ldots, n - 2$).

Der aus den Pseudozügen $M_1, M_2, \ldots, M_{n-2}$ zusammengesetzte geschlossene Teil von K hat den Index $n - 2$. Sein Index ist nämlich nicht kleiner als die Summe der Indizes von $M_1, M_2, \ldots, M_{n-2}$, also $n - 2$, und nicht größer als der Index von K; und dieser ist höchstens gleich $n - 2$. K ist daher vom Maximalindex und ihr letzter, in den Winkelräumen (e_{n-1}', f_n''), (f_n', f_1') und (f_1'', e_1'') liegende Pseudozug M_{n-1} ist paar und vom Index Null. Er ist eine Schleife.

Die $n - 1$ Pseudozüge von K haben je einen Winkelpunkt in 0. Der unpaare Pseudozug M_k ($1 \leqq k \leqq n - 2$) wird von einer Geraden g durch 0 offenbar dann und nur dann in 0 nicht geschnitten, wenn g in den die Gerade f_{k+1} enthaltenden Doppelwinkelraum (e_k, e_{k+1}) fällt. Die Gerade g schneidet also mindestens $n - 3$ der unpaaren Pseudozüge $M_1, M_2, \ldots, M_{n-2}$ in 0.

Daraus folgt, daß K von jedem Kegelschnitt E durch 0 und einen von 0 verschiedenen Punkt S des paaren Pseudozuges M_{n-1} in $2n$ oder in $2n - 2$ Punkten getroffen wird. Die algebraische Kurve K der n-ten Ordnung wird nämlich von jedem Kegelschnitt der Ebene in höchstens $2n$ (reellen) Punkten getroffen. Wir müssen also nur zeigen, daß K mindestens $2n - 2$ (reelle) Punkte mit E gemeinsam hat.

g sei die Tangente von E in 0, dann schneidet E mindestens die $n - 3$ unpaaren Pseudozüge in 0, die dort von g geschnitten werden. Nach einem bekannten v. Staudtschen Satze haben eine paare und eine unpaare oder paare ebene Kurve eine gerade Anzahl von Schnittpunkten gemeinsam (wenn diese Anzahl endlich ist). Dieser Satz gilt auch dann, wenn die Kurven endlich viele Winkelpunkte haben. Daraus folgt, daß der Kegelschnitt mindestens $n - 3$ unpaare Pseudozüge auch außerhalb von 0 schneidet.

Der Kegelschnitt E hat in 0 mindestens $n - 1$ Punkte mit K gemeinsam. Er schneidet mindestens $n - 2$ Pseudozüge außerhalb von 0, und zwar mindestens $n - 3$ unpaare Pseudozüge und den paaren Pseudozug M_{n-1}, diesen in S. E hat also mindestens $(n - 1) + (n - 2) = 2n - 3$ (reelle) Punkte mit K gemeinsam. Die Anzahl der gemeinsamen Punkte von K und E ist als gerade Zahl also mindestens $2n - 2$.

Damit ist der ausgesprochene Hilfssatz bewiesen.

---

[23]) N 3, 164—165; N 10, 494, 512—513.

Die polarreziproke Figur der Kurve K in bezug auf einen Kreis der Ebene, dessen Mittelpunkt an K keine Tangenten sendet, ist eine im Endlichen liegende einzügige Kurve Γ_n der n-ten Klasse vom Maximalklassenindex, die $n-2$ Rückkehrpunkte erster Art und die Ordnung $2n-2$ hat. Die Polare t bzw. s des Punktes 0 bzw. S bezüglich dieses Kreises ist eine $(n-1)$-fache bzw. einfache Tangente der Kurve Γ_n der n-ten Klasse.

Γ_n liegt ganz auf der eine Seite ihrer $(n-1)$-fachen Tangente t, weil sie $(2n-2)$-ter Ordnung ist, daher von t nur in den $n-1$ doppelt zu zählenden Berührungspunkten $T_0, T_1, \ldots, T_{n-2}$ getroffen wird. Die Kurve Γ_n wird durch diese Punkte in $n-1$ Bogen $B_1, B_2, \ldots, B_{n-1}$ zerlegt, von denen die ersten $n-2$ in der Polarreziprozität den $n-2$ unpaaren Pseudozügen von K entsprechen. Jeder dieser $n-2$ Bogen enthält je einen Rückkehrpunkt; der dem paaren Pseudozug von K entsprechende Bogen B_{n-1} hat keinen. B_{n-1} ist von zweiter Klasse, also konvex. Der Pseudozug M_{n-1} von K ist nämlich von zweiter Ordnung, weil eine Gerade der Ebene mit den $n-2$ unpaaren Pseudozügen mindestens $n-2$, mit dem paaren Pseudozug also höchstens 2 Punkte gemeinsam hat. Offenbar sind die Endpunkte von B_{n-1} (bei passenden Bezeichnungen) die äußersten Berührungspunkte T_0 und T_{n-2} der Kurve Γ_n mit t.

Die Gerade s berührt den Bogen B_{n-1} und schneidet t in einem außerhalb der Strecke $T_0\,T_{n-2}$ liegenden Punkte Q. Dieser Punkt liegt in demjenigen Gebiet der Ebene, dessen Punkte n Tangenten an Γ_n senden; denn s bzw. t ist als einfache bzw. $(n-1)$-fache Tangente zu rechnen. Aus Q erreicht man also die konvexe Seite der Kurve Γ_n[24]).

Γ_n schneidet daher auch s nicht. Im entgegengesetzten Falle schickte nämlich die Kurve Γ_n der n-ten Klasse mindestens noch eine Tangente durch Q. Dreht man nämlich die von Q ausgehende Halbgerade von t, die keinen Berührungspunkt enthält, um Q in die berührende Halbgerade t, so wird Γ_n von der ersten der beschriebenen Halbgeraden, von der sie überhaupt getroffen wird, notwendigerweise berührt. Γ_n hat aber nicht mehr als n von Q ausgehende Tangenten.

Aus dem Obigen ergibt sich, daß Γ_n ganz in einem Winkelraum W liegt, dessen Schenkel von s und t gebildet werden. Wir legen in einen der beiden Nebenwinkelräume von W eine Kurve Γ_m der m-ten Klasse vom Maximalklassenindex, die von der einen der Geraden s und t einfach, von der anderen aber $(m-1)$-fach berührt wird, und die ähnliche Eigenschaften hat wie Γ_n. Die $(m-1)$-fache Tangente von Γ_n kann also entweder in t oder in s fallen.

Die Kurven Γ_n und Γ_m bilden offenbar eine Kurve $(n+m)$-ter Klasse vom Maximalklassenindex. Diese hat mit jedem Kegelschnitt E', der von t und s berührt wird, höchstens $2(n+m)$ und mindestens $2(n+m)-2$ Tangenten gemeinsam, von denen $n+m$ in das Geradenpaar t und s fallen.

Bezeichnet nämlich U_2, U_n bzw. U_m das einfach zusammenhängende Gebiet der Ebene, das von der Kurve E', Γ_n bzw. Γ_m begrenzt wird, so hat U_2 nur mit einem der Gebiete U_n und U_m einen inneren Punkt gemeinsam. Haben U_2 und U_n keinen inneren Punkt gemeinsam, so haben E' und Γ_n $2n$ Tangenten gemeinsam, weil sie eine reduzible Kurve $(n+2)$-ter Klasse vom Maximalindex bilden [25]). Haben U_2 und U_n auch innere Punkte gemeinsam, so haben die Kurven E' und Γ_n nach dem Obigen mindestens $2n-2$ Tangenten gemeinsam.

Daraus folgt die Richtigkeit unserer Behauptung.

Geht man zur bezüglich eines Kreises der Ebene polaren Figur der aus Γ_m und Γ_n bestehenden Kurve über, so erhält man den Satz:

---

[24]) Eine Kurve Γ_n hat die Form der Figur 1 in der Arbeit N 9, 84.

[25]) N 4, 186—187.

Zu beliebigen ganzen Zahlen m (> 2) und n (> 2) gibt es eine aus zwei Zügen C_1 und C_2 m-ter und n-ter Ordnung bestehende reduzible ebene Kurve vom Maximalindex, die nicht nur bezüglich der Geraden, sondern auch bezüglich eines dreidimensionalen linearen Kegelschnittsystems die Ordnung $n + m$ und den Index $n + m - 2$ hat. Die Züge C_1 und C_2 haben auch in bezug auf diese Kegelschnitte die Ordnungen m und n, die Indizes $m - 2$ und $n - 2$.

5. Darstellung reduzibler Raumkurven vom Maximalindex.

Die Existenz reduzibler Raumkurven vom Maximalindex wird durch den folgenden Satz ausgedrückt:

IV. *Sind m und n ganz und größer als zwei, so gibt es eine reduzible, auf einer Regelfläche zweiter Ordnung gelegene Raumkurve $(m + n)$-ter Ordnung vom Maximalindex, die aus zwei einzügigen Kurven m-ter und n-ter Ordnung vom Maximalindex besteht.*

Dieser Satz wird auf Grund unseres zweiten Hilfssatzes über ebene algebraische Kurven vom Maximalindex bewiesen.

Wir bezeichnen mit C die aus den Zügen C_1 und C_2 m-ter und n-ter Ordnung bestehende ebene Kurve $(m + n)$-ter Ordnung vom Maximalindex und mit

$$\lambda_0 f_0(x, y) + \lambda_1 f_1(x, y) + \lambda_2 f_2(x, y) + \lambda_3 f_3(x, y) = 0 \tag{1}$$

die Gleichung des dreidimensionalen linearen Kegelschnittsystems in kartesischen Koordinaten, bezüglich dessen Kegelschnitte die Kurve C die Ordnung $m + n$ und den Index $m + n - 2$ hat.

Die Transformation

$$\xi = \frac{f_1(x, y)}{f_0(x, y)}, \quad \eta = \frac{f_2(x, y)}{f_0(x, y)}, \quad \zeta = \frac{f_3(x, y)}{f_0(x, y)} \tag{2}$$

führt die x, y-Ebene offenbar in eine Regelfläche H von zweiter Ordnung über und die ebene Kurve C in eine auf H gelegene Raumkurve G der $(m + n)$-ten Ordnung vom Maximalindex, die in zwei einzügige Raumkurven m-ter und n-ter Ordnung zerfällt.

Die veränderlichen Schnittpunkte der Kurve C mit den Kegelschnitten von (1) entsprechen nämlich eindeutig den Schnittpunkten der Kurve mit den entsprechenden Ebenen

$$\lambda_0 + \lambda_1 \xi + \lambda_2 \eta + \lambda_3 \zeta = 0.$$

Die Kurve G wird also von jeder Ebene entweder in $m + n$ oder in $m + n - 2$ Punkten getroffen.

Damit ist Satz IV vollständig bewiesen.

6. Das Geschlecht der Raumkurven vom Maximalindex.

Das *Geschlecht* der Raumkurve G n-ter Ordnung vom Maximalindex wird durch die Gleichung

$$p = \frac{(n - 1)(n - 2)}{2} - d - h$$

definiert, wo d die Anzahl der wirklichen Doppelpunkte, h die Maximalanzahl der scheinbaren Doppelpunkte von G bedeutet [26]).

Aus der Definition des Geschlechtes p ergibt sich der folgende Satz:

V. *Das Geschlecht der ebenen Projektion einer Raumkurve G vom Maximalindex (aus einem außerhalb der Kurve liegenden Punkte) ist gleich dem Geschlecht von G oder um eins größer.*

---

[26]) M 1, 175; N 3, 164—165; N 4, 179—187; N 12, 434—444.

Projizieren wir die Raumkurve G aus zwei beliebigen (außerhalb von G liegenden) Punkten S' und S'' auf eine Ebene, so erhalten wir zwei ebene Kurven C' und C'' vom Maximalindex. Diese Projektionen bestimmen zwischen den Punkten der Kurven G und C', G und C'', C' und C'' je eine umkehrbar eindeutige Zuordnung. Hierbei entspricht einer Faktorkurve der einen der Kurven G, C' und C'' je eine Faktorkurve der beiden anderen Kurven, und entsprechende Faktorkurven haben dieselbe Ordnung. G, C' und C'' zerfallen also in gleichviele irreduzible Faktorkurven.

Bezeichnen wir mit $G_1, G_2, \ldots, G_k$ die irreduziblen Faktorkurven von G, mit C_1', $C_2', \ldots, C_k'$ bzw. $C_1'', C_2'', \ldots, C_k''$ die entsprechenden irreduziblen Faktorkurven von C' bzw. C'', mit p, p', p'', p_h' bzw. p_h'' das Geschlecht der Kurve G, C', C'', C_h' bzw. C_h'' $(h = 1, 2, \ldots, k)$, so bestehen die Gleichungen [27])

$$p' = p_1' + p_2' + \cdots + p_k' - k + 1 \text{ und } p'' = p_1'' + p_2'' + \cdots + p_k'' - k + 1.$$

Da das Geschlecht einer irreduziblen ebenen Kurve vom Maximalindex gleich der Anzahl ihrer Züge vom Geschlecht Eins ist [28]), hat die Kurve C' bzw. C'' $p_1' + p_2' + \cdots + p_k'$ bzw. $p_1'' + p_2'' + \cdots + p_k''$ Züge vom Geschlecht Eins.

Die aus s Zügen bestehende und in k irreduzible Faktorkurven zerfallende Kurve C' oder C'' hat entweder k oder $k - 1$ Züge vom Geschlecht Null und deshalb entweder $s - k$ oder $s - k + 1$ Züge vom Geschlecht Eins [29]). Folglich ist das Geschlecht der Kurve C' oder C'' entweder

$$(s - k) - k + 1 = s - 2k + 1 \text{ oder } (s - k + 1) - k + 1 = s - 2k + 2.$$

C' hat somit höchstens einen Doppelpunkt mehr oder weniger als C'', das Gleiche gilt auch für die scheinbaren Doppelpunkte von G bezüglich S' und S''.

Nach Satz 1 von C. Juel gibt es Punkte S' und S'' außerhalb von G, so daß G einen scheinbaren Doppelpunkt mehr bezüglich S' als bezüglich S'' hat. Daher hat die Raumkurve G das Geschlecht $p = s + 1 - 2k$ und ihre ebene Projektion C' oder C'' das Geschlecht p oder $p + 1$.

Damit ist Satz V vollständig bewiesen.

Aus dem Beweise des Satzes V folgen die Sätze:

VI. *Die aus s Zügen bestehenden irreduziblen Raumkurven vom Maximalindex sind vom Geschlecht* $s - 1$. *Die aus s Zügen bestehenden und in k irreduzible Kurven zerfallenden Raumkurven vom Maximalindex haben das Geschlecht* $p = s + 1 - 2k$.

VII. *Die einzügigen Raumkurven haben das Geschlecht Null.*

Aus dem Satze VI folgt der Satz:

VIII. *Zerfällt eine Raumkurve vom Maximalindex vom Geschlecht p in k irreduzible Faktorkurven von den Geschlechtern* $p_1, p_2, \ldots, p_k$, *so ist*

$$p = p_1 + p_2 + \cdots + p_k - k + 1.$$

Zerfällt nämlich die aus s Zügen bestehende Raumkurve G vom Maximalindex vom Geschlecht p in k irreduzible Faktorkurven $G_1, G_2, \ldots, G_k$, und bezeichnet p_h das Geschlecht, s_h die Anzahl der Züge von G_h $(h = 1, 2, \ldots, k)$, so gelten die Relationen

$$s = s_1 + s_2 + \cdots + s_k, \; p = s - 2k + 1, \; p_h = s_h - 1 \qquad (h = 1, 2, \ldots, k).$$

Hieraus ergibt sich die Relation

$$p = p_1 + p_2 + \cdots + p_k - k + 1.$$

---

[27]) N 4, 179.

[28]) N 4, 180—181.

[29]) N 4, 181—183.

7. Einige Zusammenhänge zwischen Ordnung, Geschlecht, Anzahl der Züge und der irreduziblen Faktorkurven für die Raumkurven vom Maximalindex.

Der Satz VI läßt sich auch so fassen:

IX. *Die irreduziblen bzw. in k irreduzible Kurven zerfallenden Raumkurven von Maximalindex und vom Geschlecht p bestehen aus* $p+1$ *bzw.* $p+2k-1$ *Zügen.*

Ist p das Geschlecht einer in k irreduzible Faktorkurven zerfallenden Raumkurve n-ter Ordnung vom Maximalindex und sind $i_1, i_2, \ldots, i_s$ die Indizes der Züge der Raumkurve, so gilt

$$n = i_1 + i_2 + \cdots + i_s + 2k \quad \text{und} \quad p = s + 1 - 2k$$

(Satz II bzw. VI).

Wegen Satz 2 ist $i_h \geqq 1$ für $h = 1, 2, \ldots, s$. Aus dem Obigen folgt daher

$$n \geqq s + 2k \quad \text{und} \quad p = s - 2k + 1,$$

oder

$$n + p \geqq 2s + 1 \quad \text{und} \quad n - p \geqq 4k - 1,$$

und das Gleichheitszeichen steht dann und nur dann, wenn alle Züge der Raumkurve vom Index Eins, also von dritter Ordnung sind.

Wir haben somit:

X. *Die Summe der Ordnung und des Geschlechtes einer Raumkurve vom Maximalindex ist um mindestens* 1 *größer als die doppelte Anzahl ihrer Züge. Dieses Minimum wird genau dann angenommen, wenn alle Züge der Raumkurve von dritter Ordnung sind.*

XI. *Das Geschlecht einer Raumkurve n-ter Ordnung vom Maximalindex ist höchstens* $n-3$. *Zerfällt sie in k irreduzible Faktorkurven, so ist ihr Geschlecht höchstens* $n+1-4k$. *Das Gleichheitszeichen steht dann und nur dann, wenn alle Züge der Kurve von dritter Ordnung sind.*

XII. *Eine Raumkurve n-ter Ordnung vom Maximalindex ist immer irreduzibel, wenn ihr Geschlecht größer als* $n-7$ *ist. Ist ihr Geschlecht aber größer als* $n+1-4k$, *so zerfällt die Raumkurve in höchstens* $k-1$ *irreduzible Faktorkurven.*

Zerfällt die Raumkurve der n-ten Ordnung vom Maximalindex und vom Geschlecht p in k irreduzible Kurven von den Ordnungen $n_1, n_2, \ldots, n_k$ und von den Geschlechtern $p_1, p_2, \ldots, p_k$, so gelten offenbar die Relationen

$$n = n_1 + n_2 + \cdots + n_k \geqq 3k \quad \text{und} \quad p = p_1 + p_2 + \cdots + p_k - k + 1 \geqq -k + 1.$$

Aus diesen Ungleichungen folgt der Satz

XIII. *Das Geschlecht einer Raumkurve n-ter Ordnung vom Maximalindex ist nicht kleiner als* $-\left[\frac{n}{3}\right] + 1$. Hierbei bedeutet $\left[\frac{n}{3}\right]$ die größte ganze Zahl $\leqq \frac{n}{3}$.

Insbesondere hat keine Raumkurve höchstens fünfter Ordnung vom Maximalindex negatives Geschlecht. Es gibt aber ebene Kurven vierter Ordnung vom Maximalindex und vom Geschlecht -1.

8. Über die Anzahl der wirklichen und scheinbaren Doppelpunkte einer Raumkurve vom Maximalindex.

Man sieht den folgenden Satz leicht ein:

XIV. *Die Raumkurven vom Maximalindex haben keinen Rückkehrpunkt.*

Die Projektion einer Raumkurve G vom Maximalindex mit Rückkehrpunkten aus einem Punkte, der auf einer Tangente von G, aber nicht auf G selbst läge, wäre nämlich eine ebene Kurve vom Maximalindex mit wenigstens zwei Rückkehrpunkten. Eine ebene Kurve vom Maximalindex hat aber höchstens einen Rückkehrpunkt [30]).

[30]) N 2, 73.

Aus der Definition des Geschlechtes und den Sätzen V—IX folgen die Sätze:

XV. *Die Gesamtzahl der wirklichen und der scheinbaren Doppelpunkte bezüglich eines allgemeinen Punktes des Raumes beträgt für eine Raumkurve n-ter Ordnung vom Maximalindex und vom Geschlecht p*

$$\frac{(n-1)(n-2)}{2} - p \quad \textit{oder} \quad \frac{(n-1)(n-2)}{2} - p - 1 .$$

XVI. *Jede irreduzible bzw. in k irreduzible Kurven zerfallende und aus s Zügen bestehende Raumkurve n-ter Ordnung vom Maximalindex hat die Gesamtanzahl*

$$\frac{(n-1)(n-2)}{2} - s + 1 \quad \textit{oder} \quad \frac{(n-1)(n-2)}{2} - s$$

bzw.

$$\frac{(n-1)(n-2)}{2} - s - 1 + 2k \quad \textit{oder} \quad \frac{(n-1)(n-2)}{2} - s - 2 + 2k$$

wirklicher und scheinbarer Doppelpunkte bezüglich eines allgemeinen (außerhalb der Raumkurve liegenden) *Punktes.*

Über die Anzahl der wirklichen Doppelpunkte beweisen wir jetzt den folgenden Satz:

XVII. *Bezeichnet $G_n^{(p)}$ eine Raumkurve n-ter Ordnung vom Maximalindex und vom Geschlecht p, so sind die Kurven $G_3^{(0)}, G_4^{(1)}, G_5^{(2)}, \ldots, G_n^{(n-3)}$ doppelpunktfrei. Die Kurven $G_4^{(0)}$ und $G_5^{(1)}$ haben höchstens einen, die Kurven $G_5^{(0)}$ höchstens zwei Doppelpunkte.*

Die Raumkurven $G_n^{(n-3)}$ sind irreduzibel und besitzen $n-2$ Züge dritter Ordnung. Kein Zug dritter Ordnung hat einen Doppelpunkt. Andernfalls träfe nämlich eine Ebene durch den Doppelpunkt und noch zwei Punkte des Zuges ihn in mehr als drei Punkten. Haben zwei Züge dritter Ordnung M_1 und M_2 einer Raumkurve vom Maximalindex einen Punkt gemein, so bilden sie eine Raumkurve sechster Ordnung. Haben nämlich die Züge M_1 und M_2 den Schnittpunkt P, so schneidet eine durch P und durch je einen anderen Punkt von M_1 und M_2 hindurchgehende Ebene beide Züge in je drei Punkten, weil sie mit den unpaaren Zügen M_1 und M_2 je eine ungerade Anzahl gemeinsamer Punkte hat.

Daraus folgt der Satz XVII für die Kurven $G_n^{(n-3)}$, weil je zwei Züge einer irreduziblen Raumkurve vom Maximalindex eine irreduzible Kurve bilden (Satz III).

Die Kurven $G_4^{(0)}$ haben höchstens einen Doppelpunkt. Hätte nämlich eine Kurve $G_4^{(0)}$ mindestens zwei Doppelpunkte, so hätte sie mit einer Ebene durch die zwei Doppelpunkte und einen dritten Punkt der Kurve mehr als vier Schnittpunkte.

Die Kurven $G_5^{(0)}$ haben höchstens zwei Doppelpunkte. Eine Kurve $G_5^{(0)}$ mit drei oder mehr Doppelpunkten würde nämlich von einer Ebene durch drei Doppelpunkte in mindestens sechs Punkten getroffen werden.

Jede Kurve $G_5^{(1)}$ besteht aus einem Zug M_1 dritter und aus einem M_2 vierter Ordnung. Die Züge M_1 und M_2 haben höchstens einen Punkt gemeinsam. Hätten sie nämlich mindestens zwei Punkte gemeinsam, so träfe die Kurve $G_5^{(1)}$ eine Ebene durch diese Punkte und einen dritten Punkt auf M_2 in mindesten $3 + 4 = 7$ Punkten. Hätte nun der Zug M_2 einen Doppelpunkt und einen gemeinsamen Punkt mit M_1, so schnitte eine Ebene durch diese zwei Punkte und einen weiteren Punkt von M_1 die Kurve $G_5^{(1)}$ ebenfalls in mindestens 7 Punkten. (Daß M_2 nicht zwei Doppelpunkte hat, ist klar.)

Damit ist der Satz XVII vollständig bewiesen.

Ferner gilt der Satz:

XVIII. *Eine einzügige Raumkurve n-ter Ordnung* $(n > 3)$ *vom Maximalindex hat höchstens* $\frac{(n-3)(n-4)}{2} + 1$ *Doppelpunkte.*

Die Projektion einer einzügigen Raumkurve G der n-ten Ordnung vom Maximalindex aus einem Doppelpunkt P auf eine Ebene ε ist eine einzügige ebene Kurve C der $(n-2)$-ten Ordnung vom Maximalindex. Dem Doppelpunkte P entsprechen die beiden Punkte von C, in denen die zwei Tangenten von P die Ebene ε schneiden. Den übrigen Doppelpunkten von G entsprechen ebenfalls Doppelpunkte von C.

Die Kurve C hat das Geschlecht Null oder Eins, sie hat also

$$\frac{(n-3)(n-4)}{2} \quad \text{oder} \quad \frac{(n-3)(n-4)}{2} - 1$$

Doppelpunkte [31]). Für die Anzahl der Doppelpunkte von G (einschließlich des Doppelpunktes P) gilt also Satz XVIII.

Wir beweisen weiter:

XIX. *Bilden die Züge* M_1 *und* M_2 *der* n_1*-ten und* n_2*-ten Ordnung eine zweizügige irreduzible Raumkurve vom Maximalindex, so haben sie höchstens* $(n_1-3)(n_2-3)+1$ *Punkte gemeinsam. Ist* $n_1 = n_2 = 3$*, so haben sie keinen Punkt gemeinsam.*

Ist nämlich P ein gemeinsamer Punkt der Züge M_1 und M_2, so ist die Projektion von M_1 bzw. M_2 aus P auf eine Ebene ε eine einzügige ebene Kurve N_1 bzw. N_2 der (n_1-1)-ten bzw. (n_2-1)-ten Ordnung. Dem Punkte P entsprechen die beiden Punkte von N_1 und N_2, in denen die Tangenten der Züge M_1 und M_2 in P die Ebene ε schneiden. Jedem anderen Schnittpunkte von M_1 und M_2 entspricht ein Schnittpunkt von N_1 und N_2.

Man sieht leicht ein, daß die Züge N_1 und N_2 eine irreduzible ebene Kurve vom Maximalindex bilden. Daraus folgt, daß die Anzahl der Schnittpunkte von N_1 und N_2 gleich dem Produkt der Indizes dieser Züge, also gleich $(n_1-3)(n_2-3)$ ist [32]). Die Anzahl der gemeinsamen Punkte von M_1 und M_2 ist um höchstens 1 größer.

Damit ist Satz XIX bewiesen, denn nach dem Beweise des Satzes XVII können die Züge M_1 und M_2 im Falle $n_1 = n_2 = 3$ keinen Punkt gemeinsam haben.

Ferner gilt Satz

XX. *Eine reduzible Raumkurve G vom Maximalindex zerfalle in zwei Faktorkurven* G_1 *und* G_2 *der* n_1*-ten und* n_2*-ten Ordnung; dann haben diese nicht mehr als* $(n_1-1)(n_2-1)+1$ *Punkte gemeinsam.*

Der Punkt P sei G_1 und G_2 gemeinsam; wir projizieren die Kurve G aus P auf eine (P nicht enthaltende) Ebene ε. Hierbei gehen G_1 und G_2 in zwei Kurven C_1 und C_2 der (n_1-1)-ten und (n_2-1)-ten Ordnung über, die zusammen eine reduzible ebene Kurve vom Maximalindex bilden. Die Anzahl der Schnittpunkte von C_1 mit C_2 ist daher gleich dem Produkte ihrer Ordnungen [33]). Da die Projektion jeden Schnittpunkt von G_1 und G_2 außer P in einen Schnittpunkt von C_1 und C_2 überführt, schneiden sich die Raumkurven G_1 und G_2 in höchstens $(n_1-1)(n_2-1)+1$ Punkten.

Aus den Sätzen XVIII und XIX folgt schließlich:

---

[31]) N 3, 165; N 4, 179—182.

[32]) N 4, 183—184, 186—187.

[33]) N 4, 185—187.

XXI. *Eine aus s Zügen bestehende irreduzible Raumkurve n-ter Ordnung vom Maximalindex hat höchstens*

$$\frac{s(s+1)}{2} - \frac{a(a+1)}{2} + \frac{(n-2-s)(n-3-s)}{2}$$

Doppelpunkte; hierbei bedeutet a die Anzahl der Züge dritter Ordnung.

Die irreduzible Raumkurve G der Ordnung n vom Maximalindex bestehe aus den Zügen $M_1, M_2, \ldots, M_s$ der Ordnungen $n_1, n_2, \ldots, n_s$. Dann ist

$$n = (n_1 - 2) + (n_2 - 2) + \cdots + (n_s - 2) + 2 = n_1 + n_2 + \cdots + n_s - 2s + 2.$$

Die d Doppelpunkte der Kurve G sind teils Doppelpunkte der Züge, teils Schnittpunkte von je zwei Zügen. Auf Grund der Sätze XVIII und XIX folgt also die Ungleichung

$$(3) \quad d \leqq \sum_{h=1,2,\ldots,s} \left[\frac{(n_h-3)(n_h-4)}{2} + 1\right] + \sum_{h,j=1,2,\ldots,s;\, h<j} [(n_h-3)(n_j-3)+1].$$

Hieraus erhalten wir durch entsprechende Umformung die Ungleichung

$$(4) \qquad d \leqq \frac{s(s+1)}{2} + \frac{(n-2-s)(n-3-s)}{2}.$$

a der s Züge von G seien von dritter Ordnung; diese Züge sind doppelpunktfrei und schneiden sich nicht. Die Ungleichung (3) bleibt daher richtig, wenn man die erste Summe der rechten Seite um a, die zweite um $\frac{a(a-1)}{2}$, die ganze rechte Seite also um $\frac{a(a+1)}{2}$ verkleinert. Die Ungleichung (4) bleibt also richtig, wenn man ihre rechte Seite um $\frac{a(a+1)}{2}$ verkleinert.

Damit ist der Satz XXI bewiesen. Dieser Satz läßt sich im allgemeinen nicht verfeinern. Hat nämlich die Kurve nur Züge dritter Ordnung, so hat sie keinen Doppelpunkt, wie es auch aus dem Satze XXI folgt.

Durch einen ähnlichen Beweisgang, wie den der Sätze XVIII—XX, kann man entsprechende Sätze für die Fälle ableiten, daß ein Zug einen q-fachen Punkt hat oder daß ein Schnittpunkt zweier Züge auf dem einen Zug q_1-fach, auf dem anderen q_2-fach zu zählen ist. Der Satz XXI läßt sich auf reduzible Kurven übertragen.

9. Die Klasse und der Rang einer Raumkurve vom Maximalindex.

Die *Klasse* bzw. der *Klassenindex* einer Raumkurve G ist die größte bzw. kleinste Zahl der Schmiegebenen von G durch einen Punkt des Raumes.

Aus der Definition folgt, daß die Klasse bzw. der Klassenindex der Raumkurve gleich der Maximal- bzw. Minimalanzahl der Wendepunkte der ebenen Projektionen von G ist.

Die ebene Projektion einer Raumkurve vom Maximalindex und vom Geschlecht p aus einem allgemeinen Punkte des Raumes hat das Geschlecht p oder $p+1$ und deshalb $n+2p-2$ oder $n+2p$ Wendepunkte. Denn eine ebene Kurve n-ter Ordnung vom Maximalindex und vom Geschlecht p hat $n+2p-2$ Wendepunkte [34]).

Daraus folgen die Sätze:

XXII. *Die Raumkurven vom Maximalindex sind auch vom Maximalklassenindex.*

[34]) N 3.

XXIII. *Geht die maximale bzw. minimale Anzahl der Doppelsekanten einer Raumkurve n-ter Ordnung vom Maximalindex und vom Geschlecht p durch einen Punkt P des Raumes, so gehen* $n + 2p - 2$ *bzw.* $n + 2p$ *Schmiegebenen der Raumkurve durch P.*

XXIV. *Die Klasse bzw. der Klassenindex einer Raumkurve vom Maximalindex und vom Geschlecht Null ist gleich ihrer Ordnung bzw. ihrem Index.*

Der *Rang* einer Raumkurve G ist die Maximalanzahl der Tangenten von G, die eine beliebige Gerade des Raumes schneiden.

P sei der Schnittpunkt der Geraden p mit einer Ebene ε, C die Projektion der Raumkurve in der Ebene ε aus einem Punkte P^* von p; dann entsprechen die Tangenten von C durch P eindeutig denen von G, die die Gerade p schneiden.

Der Rang der Raumkurve G ist also die Maximalklasse ihrer ebenen Projektionen.

Eine ebene Kurve n-ter Ordnung vom Maximalindex und vom Geschlecht p hat höchstens die Klasse [34])

$$2n - 2 + 2p - r = n(n-1) - 2d - 3r,$$

wo d die Anzahl der Doppelpunkte, r die Anzahl der Rückkehrpunkte bedeutet.

Daraus folgt der Satz:

XXV. *Der Rang einer Raumkurve n-ter Ordnung vom Maximalindex und vom Geschlecht p ist höchstens* $2n + 2p - 2$.

10. Über die Deformation der Raumkurven vom Maximalindex in solche ohne Doppelpunkte. Raumkurven ohne Singularitäten.

Wir nehmen an, die Raumkurve G vom Maximalindex habe im Punkte P einen Doppelpunkt, der auf den Bogen γ_1 und γ_2 liege. Wir bezeichnen die Tangenten von γ_1 und γ_2 in P mit p_1 und p_2. Ferner bezeichnen wir die Projektion von G aus einem Punkte S_1 von p_1 auf eine Ebene ε mit C, die von P, p_2, γ_1 und γ_2 der Reihe nach mit Q, q_2, δ_1 und δ_2; C ist vom Maximalindex. Die Bogen γ_1 und γ_2 können offenbar so klein gewählt werden, daß die Bogen δ_1 und δ_2 keinen Punkt außer Q gemeinsam haben.

Wir können annehmen, daß die Kurve G sich im Punkte P nicht berührt, d. h. daß die Geraden p_1 und p_2 nicht zusammenfallen. Nach dieser Annahme ist also q_2 kein Punkt, sondern eine Gerade.

Berührt sich nämlich G in P, so ist Q ein gemeinsamer Rückkehrpunkt von δ_1 und δ_2. Die Tangenten t_1 und t_2 dieser Rückkehrpunkte sind die Schnittgeraden der Ebene ε mit den Schmiegebenen von γ_1 und γ_2 in P. Fallen nun die Geraden t_1 und t_2 nicht zusammen, so kann man in der Ebene ε eine Gerade g durch Q ziehen, die nur die vier in Q zusammenfallenden Punkte mit δ_1 und δ_2 in der Nähe von Q gemeinsam hat. Dann gibt es aber in jeder beliebigen Umgebung von g eine nicht durch Q gehende Gerade f, die vier Punkte weniger mit C gemeinsam hat als g.

Fallen auch die Geraden t_1 und t_2 zusammen, so hat t_1 insgesamt sechs Punkte in Q mit den Bogen δ_1 und δ_2 gemeinsam. Es gibt also in der Umgebung von t_1 eine Gerade, die vier Punkte weniger mit C gemeinsam hat als t_1.

In jedem der beiden Fälle gibt es also zwei Geraden, so daß die eine C in vier Punkten weniger trifft als die andere. Dies ist aber unmöglich, weil C vom Maximalindex ist.

Daraus folgt der Satz:

XXVI. *Eine Raumkurve vom Maximalindex hat keinen Selbstberührungspunkt.*

---

[35]) N 9; N 10.

Aus dem Beweise folgt, daß die Projektion der Tangente p_2 von γ_2 eine Gerade q_2 ist, von der δ_2 in Q berührt wird. Der Punkt Q ist Rückkehrpunkt von δ_1. Die Tangente dieses Rückkehrpunktes ist die Schnittgerade der Ebene ε mit der Schmiegebene von γ_1 in P.

Q ist ein gewöhnlicher Punkt von δ_2. Wäre nämlich Q ein Wendepunkt von δ_2, so gäbe es in beliebiger Nähe von q_2 eine Gerade f der Ebene ε, die vier Punkte weniger mit C gemeinsam hat als q_2.

Aus demselben Grunde liegt der Bogen δ_1 auf der konvexen Seite von δ_2.

Die Tangente q_2 von δ_2 fällt nicht mit der Tangente t_1 von δ_1 im Rückkehrpunkte zusammen. (Andernfalls gäbe es in beliebiger Nähe von t_1 eine Gerade f, die den Bogen δ_1 und δ_2 in der Umgebung von Q in einem bzw. keinem Punkte schneidet. Die Gerade f hätte also vier Punkte weniger mit C als t_1.) Läge nun δ_1 auf der konkaven Seite von δ_2, so träfe eine passende Gerade keinen der Bogen δ_1 und δ_2 in der Umgebung von Q. Diese Gerade hätte vier Punkte weniger mit C als q_2.

Man sieht leicht ein, daß, falls auch ein dritter Bogen γ_3 von G durch den mehrfachen Punkt P geht, δ_1 ebenfalls auf der konvexen Seite des entsprechenden Bogens δ_3 liegt. Hierbei bedeutet δ_3 die ebene Projektion des genügend kleinen Bogens γ_3.

Wir ersetzen jetzt den Bogen δ_2 durch einen (mit stetigen Tangenten versehenen) Konvexbogen δ_2^* mit denselben Endpunkten und Endtangenten, der dem Bogen δ_2 hinreichend nahe liegt und mit δ_1 in der Umgebung von Q zwei Punkte Q_1 und Q_2 gemeinsam hat. Q liegt also auf der konkaven Seite von δ_2^*.

Durch eine solche Ersetzung von δ_2 läßt sich die Kurve C n-ter Ordnung vom Maximalindex in eine Kurve C^* derselben Ordnung und vom selben Index überführen.

Bezeichnet T bzw. T^* das Konvexgebiet, das vom Konvexbogen δ_2 bzw. δ_2^* und von der Verbindungsstrecke ihrer gemeinsamen Endpunkte begrenzt wird, so können wir annehmen, daß T ein Teilgebiet von T^* ist.

Eine Gerade g durch einen Punkt von T hat mit δ_2 und δ_2^*, daher auch mit C und C^* offenbar dieselbe Anzahl von Punkten gemeinsam. Hat die Gerade g keinen Punkt mit T^* gemeinsam, so trifft sie die Kurven C und C^* in denselben Punkten. Es ist klar, daß jede andere Gerade f der Ebene, die also durch einen Punkt von T^*, aber durch keinen Punkt von T geht, den Bogen δ_2^* bzw. δ_2 in zwei bzw. keinen Punkten schneidet. Keine dieser Geraden f geht durch Q.

Da C keine Doppeltangente hat, kann man den Bogen δ_2 so klein und δ_2^* dem Bogen δ_2 so nahe wählen, daß δ_2^* von keiner außerhalb von δ_2 berührenden Tangente von C geschnitten wird. Eine Gerade f (durch einen Punkt von T^*, aber durch keinen Punkt von T) läßt sich durch eine genügend kleine Drehung in eine Tangente von δ_2 überführen, so daß die Anzahl der gemeinsamen Punkte von f mit C^* bzw. C während dieser Drehung nicht geändert bzw. um zwei vergrößert wird. Die Kurve C n-ter Ordnung und vom Maximalindex wird von einer Tangente in n Punkten getroffen. Daraus folgt, daß auch C^* die Ordnung n und den Index $n-2$ hat.

Es ist leicht einzusehen, daß die Kurven C und C^* auch dann dieselbe Ordnung und denselben Index haben, wenn das Gebiet T auch solche Punkte hat, die außerhalb von T^* liegen. In diesem Falle gibt es auch solche Geraden f, von denen die Kurve C in n, die Kurve C^* aber in $n-2$ Punkten getroffen wird. Der Bogen δ_2^* kann auch ein Kegelschnittbogen sein.

Der Bogen γ_1 der Raumkurve G schneidet die Kegelfläche F durch δ_2^* und mit der Spitze S_1 in zwei Punkten P_1 und P_2, deren Projektionen aus S_1 die Punkte Q_1 und Q_2

sind. P_1 und P_2 lassen sich auf F durch einen Bogen γ_2^* dritter Ordnung verbinden, so daß γ_2^* und γ_2 in ihren gemeinsamen Endpunkten dieselben Tangenten und Schmiegebenen haben und daß γ_2^* die kleinste Verbindungslinie von P_1 und P_2 auf F in einem inneren Punkte schneidet.

(γ_2^* kann auch ein Bogen einer algebraischen Raumkurve dritter Ordnung sein. Dann ist der Bogen δ_2^* ein Kegelschnittbogen und F ein Teil einer algebraischen Kegelfläche, die wir mit $\bar{F}$ bezeichnen werden. Ist S' der von γ_2 abliegende Schnittpunkt der Fläche $\bar{F}$ mit der Schnittgeraden der Schmiegebenen von G in den Endpunkten von γ_2 und bezeichnet F' die algebraische Kegelfläche zweiter Ordnung mit der Spitze S', die von den Endtangenten von γ_2 berührt wird und durch einen inneren Punkt der kleinsten Verbindungslinie der Punkte P_1 und P_2 auf F geht, so schneiden $\bar{F}$ und F' einander in einer Raumkurve dritter Ordnung, dessen Teilbogen zwischen den Endpunkten von γ_2 ein Bogen γ_2^* ist.)

Durch eine solche Deformation des genügend kleinen Bogens von γ_2 in einen entsprechenden Bogen γ_2^* kann man die Raumkurve G der n-ten Ordnung vom Maximalindex offenbar in eine Raumkurve G^* der n-ten Ordnung vom Maximalindex überführen, die einen Doppelpunkt weniger hat als G.

Durch Fortsetzung dieses Verfahrens erhält man also den Satz:

XXVII. *Jede Raumkurve n-ter Ordnung vom Maximalindex mit Doppelpunkten läßt sich durch stetige Deformationen ihrer Bogen in eine doppelpunktfreie Raumkurve n-ter Ordnung vom Maximalindex überführen.*

Eine doppelpunktfreie Raumkurve vom Maximalindex hat nach den Sätzen 3 und XIV überhaupt keine Singularitäten, d. h. keine stationären Punkte, Tangenten und Schmiegebenen, keine Doppelpunkte und Rückkehrpunkte und keine doppeltberührenden Ebenen.

Man sieht den folgenden Satz [36]) leicht ein:

XXVIII. *Eine einzügige Raumkurve ohne irgendeine Singularität ist immer vom Maximalindex.*

Ist R diese Raumkurve, so hat sie mit der Schmiegebene π ihres Punktes P drei (und nicht mehr) in P fallende Punkte und außerdem nur einfache Schnittpunkte gemeinsam. Beschreibt nun P die Kurve R, so ändert sich die Anzahl n der gemeinsamen Punkte von R und π nicht. Andernfalls hätte R mindestens eine Singularität. Aus demselben Grunde wird R von jeder Ebene durch die Tangente von P in ebenfalls n Punkten getroffen, von denen zwei oder drei in P fallen, die übrigen einfache Schnittpunkte sind.

Bewegt sich nun eine Ebene ε im Raume, so ändert sich die Anzahl ihrer gemeinsamen Punkte mit R nur dann, wenn ε durch eine Tangente von R geht. Daraus folgt, daß R von n-ter Ordnung und vom Index $n-2$ ist.

Aus diesem Beweis folgt der Satz

XXIX. *Die Züge jeder mehrzügigen singularitätenfreien Raumkurve sind Raumkurven vom Maximalindex. Die Tangentialebenen eines Zuges haben mit der Raumkurve dieselbe Anzahl von Punkten gemeinsam.*

---

[36]) Dieser Satz wurde vom Herrn P. Scherk in einem Briefe an uns vermutet.

(Wir behaupten nicht, daß jede mehrzügige singularitätenfreie Raumkurve den Maximalindex hat).

Für die ebenen Kurven läßt sich der folgende Satz leicht einsehen:

XXX. *Eine k-zügige und singularitätenfreie ebene Kurve hat die Ordnung und Klasse $2k$ und den Index und Klassenindex Null.*

Eine einzügige und singularitätenfreie ebene Kurve ist, wie bekannt, ein Oval. Eine aus k Ovalen bestehende ebene Kurve hat dann und nur dann keinen Doppelpunkt und keine Doppeltangente, wenn die Ovale ineinander liegen. Das zweite Oval liegt nämlich im Innern des ersten, das dritte im Innern des zweiten usw. Eine aus solchen k Ovalen bestehende Kurve ist offenbar $2k$-ter Ordnung und Klasse und vom Index und Klassenindex Null.

Eingegangen 17. November 1936.

Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten.

Nach einer brieflichen Mitteilung von *F. K. Schmidt* in Jena,
bearbeitet von *H. Hasse* in Göttingen.

F. K. Schmidt an H. Hasse (25. Mai 1936):

„Vielleicht interessiert es Sie, daß ich mir die von Ihnen unlängst entwickelte Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper kurz vor Erscheinen Ihrer Arbeit [1]) in etwas anderer Form für meine gegenwärtige Vorlesung ebenfalls überlegt hatte. Mein Ziel war, diese Differentialquotienten sogleich im Großen einzuführen. Ich ging also nicht wie Sie von der Potenzreihenentwicklung an einer Stelle aus, weil ich gerne das Rechnen an der definierenden Gleichung vermeiden wollte, das dann beim Übergang vom Kleinen zum Großen erforderlich ist. Aus der Schlußbemerkung Ihrer Abhandlung ersah ich später, daß auch O. Teichmüller eine Erklärung der höheren Differentialquotienten aufgestellt hat, die von vornherein im Großen verläuft, und ich nahm daher ohne weiteres an, daß meine Definition mit der Teichmüllers übereinstimme. Die soeben erschienene Arbeit Teichmüllers [2]) überzeugt mich aber, daß das doch nicht der Fall ist. Da meine Definition im Rahmen der Theorie der algebraischen Funktionen rasch zu den benötigten Ergebnissen führt, möchte ich sie Ihnen kurz mitteilen."

Ich gebe im folgenden eine freie ausführliche Bearbeitung dieser Mitteilung, bei der ich in einigen Punkten von der ursprünglichen Beweisführung abweiche.

Nach Beendigung des Satzes fand F. K. Schmidt eine weitere Verbesserung und Verallgemeinerung der Theorie. Siehe den längeren „Zusatz bei der Korrektur", S. 223—237.

---

1. Vorbereitung.

Sei K ein separabel erzeugbarer algebraischer Funktionenkörper einer Unbestimmten über einem beliebigen Körper k als Konstantenkörper.

Ist

$$K = k(x, y) \quad \text{mit} \quad f(x, y) = 0$$

eine Erzeugung von K/k, so definieren wir einen algebraischen Funktionenkörper $\mathfrak{K}$ einer Unbestimmten über K als Konstantenkörper durch die formal gleiche Erzeugung:

$$\mathfrak{K} = K(\xi, \eta) \quad \text{mit} \quad f(\xi, \eta) = 0.$$

Dieser Körper $\mathfrak{K}$ enthält den zu K bzgl. k isomorphen Teilkörper

$$\mathsf{K} = k(\xi, \eta) \quad \text{mit} \quad f(\xi, \eta) = 0$$

und ist (nachdem er konstruiert ist) als Kompositum von K und K darstellbar:

$$\mathfrak{K} = K\,\mathsf{K}.$$

---

[1]) H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik, Journ. f. Math. **175** (1936), 50—54.

[2]) O. Teichmüller, Differentialrechnung bei Charakteristik p, Journ. f. Math. **175** (1936), 89—99.

Der Typus von $\mathfrak{K}/k$ ist durch den Typus von K/k eindeutig bestimmt, unabhängig von der zur Konstruktion benutzten Erzeugung. Er kann beschrieben werden als das Kompositum über k zweier über k als algebraisch-unabhängig zu betrachtender Körper vom Typus K/k. Wir werden jedoch hier $\mathfrak{K}$ nicht als algebraischen Funktionenkörper zweier Unbestimmten über k, sondern nur entsprechend der obigen Konstruktion als algebraischen Funktionenkörper einer Unbestimmten über K als Konstantenkörper zu betrachten haben.

Wir legen einen festen Isomorphismus $\mathfrak{J}$ bzgl. k zwischen K und K zugrunde und verabreden zur Abkürzung der Ausdrucksweise, daß bei $\mathfrak{J}$ einander zugeordnete Elemente aus K und K immer mit einander entsprecheden lateinischen und griechischen Buchstaben bezeichnet werden.

Wir beweisen dann:

I. *Es gibt einen und nur einen Primdivisor ersten Grades $\mathfrak{P}$ von $\mathfrak{K}/K$ derart, daß für jedes Element η aus K gilt*

$$\eta \equiv y \text{ mod. } \mathfrak{P}.$$

Beweis. Sei ξ ein festes über k transzendentes Element aus K und K_ξ der Integritätsbereich derjenigen Elemente aus K, die über dem Polynomintegritätsbereich $k[\xi]$ ganz-algebraisch sind. Ferner sei $\omega_1, \ldots, \omega_n$ eine Basis von $\mathsf{K}_\xi/k[\xi]$ und

$$\text{(M)} \qquad \omega_i \omega_j = \sum_{\nu=1}^{n} g_{ij\nu}(\xi)\, \omega_\nu \qquad (g_{ij\nu}(\xi) \text{ in } k[\xi])$$

ihr Multiplikationsschema. Dann ist $\mathsf{K}_\xi/k[\xi]$ eindeutig charakterisiert als ein $k[\xi]$-Modul mit der Basis $\omega_1, \ldots, \omega_n$, in dem eine Multiplikation nach dem Schema (M) besteht.

ξ ist auch ein über K transzendentes Element aus $\mathfrak{K}$, und $\omega_1, \ldots, \omega_n$ auch eine Basis für $\mathfrak{K}_\xi/K[\xi]$, wo $\mathfrak{K}_\xi$ der Integritätsbereich derjenigen Elemente aus $\mathfrak{K}$ ist, die über dem Polynomintegritätsbereich $K[\xi]$ ganz-algebraisch sind. Daher ist $\mathfrak{K}_\xi/K[\xi]$ eindeutig charakterisiert als ein $K[\xi]$-Modul mit der Basis $\omega_1, \ldots, \omega_n$, in dem eine Multiplikation nach dem Schema (M) besteht.

Nach den Grundlagen der arithmetischen Theorie der algebraischen Funktionenkörper einer Unbestimmten[3]) genügt es zum Beweis von I, zu zeigen, daß es ein und nur ein Primideal $\mathfrak{P}_\xi$ von $\mathfrak{K}_\xi/K[\xi]$ derart gibt, daß für jedes Element η aus K_ξ gilt

$$\eta \equiv y \text{ mod. } \mathfrak{P}_\xi.$$

Anders gesagt bedeutet dies, daß sich der Isomorphismus $\mathfrak{J}$ von K auf K eindeutig zu einem Homomorphismus von $\mathfrak{K}_\xi$ auf K fortsetzt.

Nun setzt sich $\mathfrak{J}$ zunächst eindeutig zu einem Homomorphismus von $K[\xi]$ auf K fort, indem jedem Polynom $F(\xi)$ über K das Element $F(x)$ aus K zugeordnet wird; daß so wirklich ein Homomorphismus entsteht, folgt ohne weiteres aus der Transzendenz von ξ über K. Der so gewonnene Homomorphismus von $K[\xi]$ auf K setzt sich dann weiter eindeutig zu einem Homomorphismus von $\mathfrak{K}_\xi$ auf K fort, indem jedem Element $\sum_{\nu=1}^{n} F_\nu(\xi)\, \omega_\nu$ aus $\mathfrak{K}_\xi$ das Element $\sum_{\nu=1}^{n} F_\nu(x)\, w_\nu$ aus K zugeordnet wird; daß so wirklich ein Homomorphismus entsteht, folgt aus der angegebenen Charakterisierung von $\mathfrak{K}_\xi/K[\xi]$, wenn man noch beachtet, daß das Multiplikationsschema (M) bei der angegebenen Fortsetzung einfach den Isomorphismus $\mathfrak{J}$ erfährt, weil es ganz innerhalb K verläuft.

Damit ist I bewiesen.

---

[3]) Siehe etwa §§ 3, 4 in F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p, Math. Zeitschr. **33** (1931), 1—32.

Wir brauchen noch eine zusätzliche Tatsache, nämlich:

II. *Ist x irgendein separierendes Element für K/k, so ist $\xi - x$ genau durch die erste Potenz von $\mathfrak{P}$ teilbar (also ein Primelement zu $\mathfrak{P}$).*

Beweis. Ist x separierend für K/k, existiert also eine Erzeugung $K = k(x, y)$ mit in y irreduzibler separabler Grundgleichung $f(x, y) = 0$, so ist die Differente $f_y(\xi, \eta)$ für $\mathfrak{R}/K(\xi)$ des Elements η, das nach I für $\mathfrak{P}$ ganz ist, durch $\mathfrak{P}$ nicht teilbar; denn nach I ist $f_y(\xi, \eta) \equiv f_y(x, y)$ mod. $\mathfrak{P}$, und nach Voraussetzung ist $f_y(x, y) \neq 0$. Daher ist $\mathfrak{P}$ unverzweigt über $K(\xi)$, und somit $\mathfrak{P}$ im Zählerprimdivisor von $\xi - x$ in $K(\xi)$ genau zur ersten Potenz enthalten.

Damit ist II bewiesen.

Wir werden gestützt auf die Tatsachen I, II die Differentialquotienten beliebiger Ordnung eines beliebigen Elements y aus K nach einem für K/k separierenden Element x definieren. Für einen vollkommenen Konstantenkörper k ist bekanntlich jedes über k transzendente Element aus K separierend für K/k.

2. Theorie der Differentialquotienten im Großen.

Es sei x irgendein separierendes Element für K/k und y ein beliebiges Element aus K. Nach I, II besteht dann eine eindeutige Potenzreihenentwicklung

$$\eta = \sum_{\varkappa=0}^{\infty} y_\varkappa (\xi - x)^\varkappa, \qquad y_\varkappa \text{ in } K,$$

nämlich einfach die $\mathfrak{P}$-adische Entwicklung von η nach dem Primelement $\xi - x$ zu $\mathfrak{P}$ mit Koeffizienten aus dem durch K eindeutig repräsentierten Restklassenkörper von $\mathfrak{P}$.

Insbesondere ist $y_0 = y$, so daß die Entwicklung auch in der Form

$$\eta - y = \sum_{\varkappa=1}^{\infty} y_\varkappa (\xi - x)^\varkappa, \qquad y_\varkappa \text{ in } K$$

geschrieben werden kann.

Wir sehen diese Entwicklung als rein-algebraisches Äquivalent der aus der Analysis bekannten Taylorentwicklung an und definieren demgemäß:

Definition.

$$\frac{d^\varkappa y}{dx^\varkappa} = y_\varkappa \qquad (\varkappa = 0, 1, 2, \dots).$$

Die so definierten Differentialquotienten sind nicht das genaue Äquivalent zu den Differentialquotienten $\frac{d^\varkappa y}{dx^\varkappa}$ der Analysis, sondern vielmehr zu den Taylorkoeffizienten $\frac{1}{\varkappa!}\frac{d^\varkappa y}{dx^\varkappa}$ der Analysis; wir können wohl trotzdem ohne Mißverständnis die Bezeichnung so wählen.

Die $\frac{d^\varkappa y}{dx^\varkappa}$ sind ihrer Definition nach durch x und y eindeutig bestimmte Elemente aus K, unabhängig von der Wahl des Isomorphismus $\mathfrak{J}$ von K auf K und dem dadurch bestimmten Primdivisor $\mathfrak{P}$ von $\mathfrak{R}/K$. Ist nämlich $\mathfrak{J}'$ ein anderer Isomorphismus von K auf K und $\mathfrak{P}'$ der zugeordnete Primdivisor von $\mathfrak{R}/K$, so unterscheiden sich $\mathfrak{J}'$ und $\mathfrak{J}$ nur durch einen Automorphismus von K/k, und $\mathfrak{P}'$ entsteht aus $\mathfrak{P}$ durch die eindeutige Fortsetzung dieses Automorphismus als solcher von $\mathfrak{R}/K$. Dabei bleiben aber die Koeffizienten $y_\varkappa$ der obigen $\mathfrak{P}$-adischen Entwicklung ungeändert.

Ferner sieht man auch, daß die $\frac{d^\varkappa y}{dx^\varkappa}$ unabhängig davon sind, ob man x, y als Elemente aus K oder aus irgendeinem separablen Erweiterungskörper K^* von endlichem

Grade über K ansieht. Denn ein Isomorphismus $\mathfrak{J}^*$ bzgl. k von K^* auf K^* enthält ja speziell einen Isomorphismus $\mathfrak{J}$ bzgl. k von K auf K, so daß dann die $\mathfrak{P}^*$-adischen Entwicklungen speziell für die Elemente aus K mit den $\mathfrak{P}$-adischen Entwicklungen dieser Elemente übereinstimmen.

Aus den Regeln für das Rechnen mit (gewöhnlichen) Potenzreihen entnimmt man ohne weiteres das Bestehen der folgenden elementaren Differentiationsregeln:

(1) *Summenregel*: $$\frac{d^\varkappa(y_1+y_2)}{dx^\varkappa}=\frac{d^\varkappa y_1}{dx}+\frac{d^\varkappa y_2}{dx}.$$

(2) *Regel für Konstantenmultiplikation*: $\dfrac{d^\varkappa(ay)}{dx^\varkappa}=a\dfrac{d^\varkappa y}{dx^\varkappa}$ für a aus k.

(3) *Produktregel*: $$\frac{d^\varkappa(y_1y_2)}{dx^\varkappa}=\sum_{\substack{\varkappa_1+\varkappa_2=\varkappa\\ \varkappa_1,\,\varkappa_2\geqq 0}}\frac{d^{\varkappa_1}y_1}{dx^{\varkappa_1}}\frac{d^{\varkappa_2}y_2}{dx^{\varkappa_2}}.$$

Ferner gilt ersichtlich speziell:

$$\frac{d^0y}{dx^0}=y,\quad \frac{d^\varkappa x}{dx^\varkappa}=\left\{\begin{matrix}x & (\varkappa=0)\\ 1 & (\varkappa=1)\\ 0 & (\varkappa>1)\end{matrix}\right\},\quad \frac{d^\varkappa a}{dx^\varkappa}=0\ (\varkappa\geqq 1)\ \text{für } a \text{ aus } k.$$

Aus der Produktregel folgt allgemeiner

(4) *Potenzregel*: $$\frac{d^\varkappa x^\mu}{dx^\varkappa}=\binom{\mu}{\varkappa}x^{\mu-\varkappa}\ (\varkappa\geqq 0),$$

zunächst für alle $\mu\geqq 0$, dann durch vollständige Induktion auch für alle $\mu<0$.

Durch Anwendung der Regeln (1)—(4) auf die Zusammensetzung eines beliebigen Polynoms $f(x,y)$ über k aus x, y und Elementen aus k ergibt sich noch leicht die spezielle Formel

$$\frac{df(x,y)}{dx}=f_x(x,y)+f_y(x,y)\frac{dy}{dx}.$$

Genügt also y der in y separablen Gleichung $f(x,y)=0$, so gilt

$$\frac{dy}{dx}=-\frac{f_x(x,y)}{f_y(x,y)}.$$

Hiernach liefert unsere allgemeine Definition speziell als erste Differentialquotienten die beim bisherigen Aufbau der arithmetischen Theorie von K/k so bezeichneten Bildungen [4]).

Auf die von mir l. c. [1]) wesentlich benutzte komplizierte allgemeine Regel für die totale Differentiation $\dfrac{d^\varkappa f(y_1,y_2)}{dx^\varkappa}$ kommt es bei unserem Aufbau nicht an; man könnte sie natürlich ebenfalls leicht aus den Regeln (1)—(3) gewinnen.

(5) *Kettenregel*: Sei t ein weiteres separierendes Element für K/k. Dann können die Differentialquotienten $\dfrac{d^\varkappa y}{dt^\varkappa}$ leicht durch die Differentialquotienten $\dfrac{d^\varkappa y}{dx^\varkappa}$ ausgedrückt werden. Für die Anwendungen kommt es nur darauf an zu wissen, daß die Formeln folgende Gestalt haben:

$$\frac{d^\varkappa y}{dt^\varkappa}=\frac{d^\varkappa y}{dx^\varkappa}g_1^{(\varkappa)}+\cdots+\frac{dy}{dx}g_\varkappa^{(\varkappa)}\qquad(\varkappa\geqq 1),$$

[4]) Siehe etwa F. K. Schmidt, l. c. [3]), § 5.

wo die $g_\lambda^{(\varkappa)}$ Polynome in $\frac{dx}{dt}, \ldots, \frac{d^\lambda x}{dt^\lambda}$ über dem Primkörper von k sind, speziell

$$g_1^{(\varkappa)} = \left(\frac{dx}{dt}\right)^\varkappa.$$

Der Beweis ergibt sich wieder aus den Regeln für das Rechnen mit Potenzreihen, indem man nämlich die $\mathfrak{P}$-adische Entwicklung

$$\eta - y = \sum_{\varkappa=1}^{\infty} \frac{d^\varkappa y}{dx^\varkappa} (\xi - x)^\varkappa$$

vermöge der $\mathfrak{P}$-adischen Entwicklung

$$\xi - x = \sum_{\varkappa=1}^{\infty} \frac{d^\varkappa x}{dt^\varkappa} (\tau - t)^\varkappa$$

auf das neue Primelement $\tau - t$ zu $\mathfrak{P}$ umrechnet; dabei muß sich ja die $\mathfrak{P}$-adische Entwicklung

$$\eta - y = \sum_{\varkappa=1}^{\infty} \frac{d^\varkappa y}{dt^\varkappa} (\tau - t)^\varkappa$$

ergeben.

3. Theorie der Differentialquotienten im Kleinen.

Sei $\mathfrak{p}$ ein Primdivisor von K/k, von dem wir vorauszusetzen haben, daß sein Restklassenkörper separabel über k ist; für einen vollkommenen Konstantenkörper k hat jeder Primdivisor $\mathfrak{p}$ von K/k diese Eigenschaft.

Es sei p ein Primelement zu $\mathfrak{p}$ und $k_\mathfrak{p}$ der innerhalb der $\mathfrak{p}$-adischen Erweiterung $K_\mathfrak{p}$ von K eindeutig bestimmte Repräsentantenköprer des Restklassenkörpers von $\mathfrak{p}$ (die in $K_\mathfrak{p}$ algebraisch-abgeschlossenee Hülle von k). Dann ist

$$K_\mathfrak{p} = \overline{k_\mathfrak{p}(p)}$$

der Körper aller (gewöhnlichen) Potenzreihen in p über $k_\mathfrak{p}$.

Wir wollen beweisen:

Satz. *Ist*

$$y = \sum_{\mu=\mu_0}^{\infty} a_\mu p^\mu, \qquad a_\mu \text{ in } k_\mathfrak{p}$$

die $\mathfrak{p}$-adische Entwicklung irgendeines Elements y aus K nach einem Primelement p zu $\mathfrak{p}$ aus K, so ist

$$\frac{d^\varkappa y}{dp^\varkappa} = \sum_{\mu=\mu_0}^{\infty} \binom{\mu}{\varkappa} a_\mu p^{\mu-\varkappa}$$

die $\mathfrak{p}$-adische Entwicklung von $\frac{d^\varkappa y}{dp^\varkappa}$.

Natürlich ist p als Primelement zu $\mathfrak{p}$ notwendig separierend für K/k; denn ein inseparierendes Element enthält jeden Primdivisor zu einem durch Char. $k\,(\neq 0)$ teilbaren Exponenten.

Daß wir hier p innerhalb K (und nicht allgemeiner innerhalb $K_\mathfrak{p}$) wählen, liegt bei unserem Aufbau in der Natur der Sache; für die Anwendungen bedeutet das keinerlei Einschränkung. Übrigens führen die Methoden unseres Beweises ohne weiteres zu einer Erweiterung der Differentiationsoperation auf beliebige Elemente aus $K_\mathfrak{p}$.

Wir brauchen aber wohl hier auf diese Seite der Sache nicht näher einzugehen, sondern können uns auf das zum Beweis unseres Satzes Nötige beschränken.

Beweis des Satzes. 1. Wegen der oben festgestellten Invarianz von $\frac{d^\varkappa y}{dp^\varkappa}$ bei separabler Erweiterung endlichen Grades von K kann $\frac{d^\varkappa y}{dp^\varkappa}$ auch in der separablen Konstantenerweiterung $Kk_\mathfrak{p}/k_\mathfrak{p}$ von K/k berechnet werden, in der die $\mathfrak{p}$-adischen Entwicklungen der Elemente aus K ihre $\mathfrak{p}^*$-adischen Entwicklungen nach einem Primdivisor ersten Grades $\mathfrak{p}^*$ von $\mathfrak{p}$ sind. Hiernach kann ohne Einschränkung von vornherein angenommen werden, daß $\mathfrak{p}$ vom ersten Grade ist, also $k_\mathfrak{p} = k$, $K_\mathfrak{p} = \overline{k(p)}$ [5]).

2. [6]) Die Behauptung des Satzes kann dann unter Beachtung der Potenzregel (4) auch so ausgesprochen werden, daß die $\mathfrak{p}$-adische Entwicklung von $\frac{d^\varkappa y}{dp^\varkappa}$ aus der $\mathfrak{p}$-adischen Entwicklung von y durch gliedweise Differentiation entsteht. Dies ergibt sich sofort, wenn die $\mathfrak{p}$-Stetigkeit der Funktion $\frac{d^\varkappa y}{dp^\varkappa}$ von y feststeht (es genügt natürlich an der Stelle 0), und diese wiederum ergibt sich, wenn man nur weiß, daß folgende Tatsache richtig ist:

(A) *Ist y ganz für $\mathfrak{p}$, so ist auch $\frac{d^\varkappa y}{dp^\varkappa}$ ganz für $\mathfrak{p}$.*

Denn dann folgt allgemeiner aus $y \equiv 0 \bmod \mathfrak{p}^\mu$, d. h. $y = p^\mu y_0$ mit für $\mathfrak{p}$ ganzen y_0, nach der Produktregel (3) und Potenzregel (4):

$$\frac{d^\varkappa y}{dp^\varkappa} = \sum_{\lambda=0}^{\varkappa} \binom{\mu}{\lambda} p^{\mu-\lambda} \frac{d^{\varkappa-\lambda} y_0}{dp^{\varkappa-\lambda}} \equiv 0 \bmod \mathfrak{p}^{\mu-\varkappa},$$

also die $\mathfrak{p}$-Stetigkeit von $\frac{d^\varkappa y}{dp^\varkappa}$ (bei 0).

3. Es ist leicht zu sehen, daß die Tatsache (A) jedenfalls für die Elemente y aus dem rationalen Funktionenkörper $k(p)$ und den $\mathfrak{p}$ enthaltenden Primdivisor $\mathfrak{p}_0$ von $k(p)$ richtig ist. Denn ist y ein Polynom in p über k, so ist $\frac{d^\varkappa y}{dp^\varkappa}$ nach den Regeln (1), (2), (4)

---

[5]) Wir tun das nur der Bequemlichkeit halber. Der nachstehende Beweis kann mit nur unwesentlichen Änderungen im Wortlaut auch ohne diese vorherige Reduktion geführt werden.

[6]) Den nachfolgenden Hauptteil des Beweises führe ich abweichend von F. K. Schmidt. Dieser ging nach dem aus der Analysis geläufigen Verfahren vor, die Potenzreihe

$$\eta = \sum_{\mu=\mu_0}^{\infty} a_\mu \pi^\mu$$

(nach trivialer Reduktion auf den Fall $\mu_0 \geqq 0$) durch die Substitution

$$\pi = p + (\pi - p)$$

formal in eine Doppelpotenzreihe nach p und $\pi - p$ umzubilden und dann mit der Definitionsreihe

$$\eta = \sum_{\varkappa=0}^{\infty} \frac{d^\varkappa y}{dp^\varkappa} (\pi - p)^\varkappa$$

zu vergleichen. Er stellt dazu fest, daß sich $\mathfrak{R}$ in den Körper $\overline{k(p,\pi)}$ aller Doppelpotenzreihen in p und π so einbetten läßt, daß dabei die Elemente y aus K in ihrer $\mathfrak{p}$-adischen Entwicklung erscheinen und die Elemente η aus K in ihrer $\mathfrak{p}$-adischen Entwicklung, wo $\mathfrak{p}$ zu $\mathfrak{p}$ durch den Isomorphismus $\mathfrak{I}$ zugeordnet ist. Und er stellt ferner fest, daß sich dabei der Primdivisor $\mathfrak{P}$ von $\mathfrak{R}/K$ zu derjenigen Bewertung von $\overline{k(p,\pi)}$ fortsetzt, die entsteht, wenn man durch $\pi = p + (\pi - p)$ formal zu Doppelpotenzreihen in p und $\pi - p$ umbildet und die kleinsten Exponenten von $\pi - p$ als Werte nimmt. Diese Feststellungen ergeben dann die Rechtfertigung des angegebenen formalen Verfahrens.

wieder ein solches, und ist $y = \frac{u}{v}$ mit Polynomen u, v in p über k, von denen v prim zu p ist, so liefert die Anwendung der Produktregel (3) auf $yv = u$ rekursiv, daß $\frac{d^\varkappa y}{dp^\varkappa}$ vom gleichen Typus ist.

Hiermit ist die Behauptung des Satzes für Elemente y aus $k(p)$ bewiesen.

Auf Grund der $\mathfrak{p}$-Stetigkeit kann für jedes Element $\bar{y}$ aus $\overline{k(p)}$ eindeutig definiert werden:

$$\text{(B)} \qquad \frac{d^\varkappa \bar{y}}{dp^\varkappa} = \mathfrak{p}_0\text{-}\lim_{i\to\infty} \frac{d^\varkappa y_i}{dp^\varkappa}, \quad \text{wenn } \bar{y} = \mathfrak{p}_0\text{-}\lim_{i\to\infty} y_i$$

irgendeine Darstellung von $\bar{y}$ als $\mathfrak{p}_0$-Grenzwert einer $\mathfrak{p}$-konvergenten Folge y_i aus $k(p)$ ist. Dabei übertragen sich ersichtlich die Regeln (1)—(3), und die neue Definition liefert speziell für Elemente y aus $k(p)$ die bisherige Bedeutung von $\frac{d^\varkappa y}{dp^\varkappa}$.

4. Wir betrachten jetzt das hyperkomplexe System $K_{\mathfrak{p}_0}/\overline{k(p)}$, das aus $K/k(p)$ durch Koeffizientenerweiterung entsteht. Es besteht aus allen Elementen

$$\bar{y} = \sum_{\nu=1}^{n} \bar{f}_\nu(p)\, w_\nu, \qquad (\bar{f}_\nu(p) \text{ in } \overline{k(p)}),$$

wo die w_ν eine Basis für $K/k(p)$ sind. In $K_{\mathfrak{p}_0}$ seien $\mathfrak{p}_0$-Konvergenz und $\mathfrak{p}_0$-Grenzwert koeffizientenweise verstanden; das hängt nicht von der Wahl der Basis w_ν ab.

Für die Elemente aus K,

$$y = \sum_{\nu=1}^{n} f_\nu(p)\, w_\nu \qquad (f_\nu(p) \text{ in } k(p)),$$

hat man die Differentiationsformel

$$\text{(C)} \qquad \frac{d^\varkappa y}{dp^\varkappa} = \sum_{\nu=1}^{n} \left(\frac{d^\varkappa f_\nu(p)}{dp^\varkappa} w_\nu + \frac{d^{\varkappa-1} f_\nu(p)}{dp^{\varkappa-1}} \frac{dw_\nu}{dp} + \cdots + f_\nu(p) \frac{d^\varkappa w_\nu}{dp^\nu} \right).$$

Stellt man hier die festen Elemente $\frac{dw_\nu}{dp_\nu}, \ldots, \frac{d^\varkappa w_\nu}{dp^\nu}$ wieder durch die Basis w_ν dar, so erkennt man, daß $\frac{d^\varkappa y}{dp^\nu}$ für die Elemente y aus K eine $\mathfrak{p}_0$-stetige Funktion ist. Daher liefert der obige Formalismus (B) wieder eine eindeutige Definition von $\frac{d^\varkappa \bar{y}}{dp^\varkappa}$ für $\bar{y}$ aus $K_{\mathfrak{p}_0}$, bei der die Regeln (1)—(3) gelten (und zwar die Produktregel (3) auch für das skalare Produkt aus einem $\overline{f(p)}$ in $\overline{k(p)}$ mit einem $\bar{y}$ in $K_{\mathfrak{p}_0}$) und bei der $\frac{d^\varkappa y}{dp^\varkappa}$ für y aus K die bisherige Bedeutung hat.

5. Sei schließlich $\bar{e}$ das zu $\mathfrak{p}$ gehörige Idempotent aus $K_{\mathfrak{p}_0}$, das also die Eigenschaft $K_{\mathfrak{p}_0}\bar{e} = \overline{k(p)}\,\bar{e}$ hat und für die Elemente y aus K durch den Mechanismus

$$y\bar{e} = f(p)\,\bar{e}$$

die zugehörigen $\mathfrak{p}$-adischen Entwicklungen $f(p)$ liefert.

Aus $\bar{e} = \bar{e}^2 = \bar{e}^3 = \cdots$ folgt nun zunächst speziell

$$\frac{d\bar{e}}{dp} = 2\bar{e}\frac{d\bar{e}}{dp} = 3\bar{e}\frac{d\bar{e}}{dp} = \cdots, \quad \text{also} \quad \frac{d\bar{e}}{dp} = 0;$$

ist ferner schon $\frac{d\bar{e}}{dp} = 0, \ldots, \frac{d^{\varkappa-1}\bar{e}}{dp^{\varkappa-1}} = 0$ bewiesen, so folgt weiter analog

$$\frac{d^{\varkappa}\bar{e}}{dp^{\varkappa}} = 2\bar{e}\frac{d^{\varkappa}\bar{e}}{dp^{\varkappa}} = 3\bar{e}\frac{d^{\varkappa}\bar{e}}{dp^{\varkappa}} = \cdots, \quad \text{also} \quad \frac{d^{\varkappa}\bar{e}}{dp^{\varkappa}} = 0\,.$$

Somit gilt allgemein

$$\frac{d^{\varkappa}\bar{e}}{dp^{\varkappa}} = 0 \qquad (\varkappa \geqq 1)\,.$$

Differenziert man die obige Darstellung des gewöhnlichen Produktes $y\bar{e}$ als skalares Produkt $f(p)\,\bar{e}$ in $K_{\mathfrak{p}_0}$ nach den für die Differentiation in $K_{\mathfrak{p}_0}$ als gültig erwiesenen formalen Regeln, so ergibt sich demnach

$$\frac{d^{\varkappa}y}{dp^{\varkappa}}\,\bar{e} = \frac{d^{\varkappa}f(p)}{dp^{\varkappa}}\,\bar{e}\,,$$

wo die Differentiation rechts als solche in $\overline{k(p)}$ gliedweise ausgeführt werden darf. Das ist, nach Fortlassen des idempotenten Faktors $\bar{e}$, die Behauptung des Satzes für beliebige y aus K.

4. Die Differentialdeterminante eines Moduls [7]).

Es sei $\mathfrak{M}$ ein k-Modul von endlichem Range n in K und x ein separierendes Element für K/k. Wir betrachten die als Hauptdivisor von der Wahl der Basis $y_0, \ldots, y_{n-1}$ von $\mathfrak{M}$ unabhängige Determinante

$$\mathfrak{d}_x(\mathfrak{M}) \cong \left|\frac{d^{\varkappa}y_i}{dx^{\varkappa}}\right| \qquad (i, \varkappa = 0, 1, \ldots, n-1)\,.$$

Bei Übergang von x zu einem anderen separierenden Element t folgt nach der Kettenregel (5)

$$\mathfrak{d}_t(\mathfrak{M}) \cong \left|\frac{d^{\varkappa}y_i}{dt^{\varkappa}}\right| = \left|\frac{d^{\varkappa}y_i}{dx^{\varkappa}}\left(\frac{dx}{dt}\right)^{\varkappa} + \frac{d^{\varkappa-1}y_i}{dx^{\varkappa-1}}\,g_2^{(\varkappa)} + \cdots + \frac{dy_i}{dx}\,g_{\varkappa}^{(\varkappa)}\right|$$
$$= \left|\frac{d^{\varkappa}y_i}{dx^{\varkappa}}\right| \cdot \left(\frac{dx}{dt}\right)^{1+2+\cdots+(n-1)} \cong \mathfrak{d}_x(\mathfrak{M}) \cdot \left(\frac{dx}{dt}\right)^{1+2+\cdots+(n-1)}.$$

Hiernach hängt der Divisor

$$\mathfrak{d}(\mathfrak{M}) = \mathfrak{d}_x(\mathfrak{M}) \cdot (dx)^{1+2+\cdots+(n-1)} \cong \left|\frac{d^{\varkappa}y_i}{dx^{\varkappa}}\right| \cdot (dx)^{1+2+\cdots+(n-1)}$$

aus der $1 + 2 + \cdots + (n-1)$-ten Potenz der Differentialklasse von K/k nur von $\mathfrak{M}$ ab, nicht von der Wahl des Elements x und der Wahl der Basis y_i. Man bezeichnet ihn mit Hinblick auf die Unabhängigkeit von x auch kurz mit

$$\mathfrak{d}(\mathfrak{M}) \cong |d^{\varkappa}y_i|\,.$$

Der Beitrag $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{M})$ eines Primdivisors $\mathfrak{p}$ von K/k (mit separablem Restklassenkörper) zu $\mathfrak{d}(\mathfrak{M})$ bestimmt sich nach Wahl eines Primelements p zu $\mathfrak{p}$, weil dp prim zu $\mathfrak{p}$ ist, als

$$\mathfrak{d}_{\mathfrak{p}}(\mathfrak{M}) = \left|\frac{d^{\varkappa}y_i}{dp^{\varkappa}}\right|_{\mathfrak{p}} = \mathfrak{d}_{\mathfrak{p}}(\mathfrak{M})_{\mathfrak{p}}\,,$$

d. h. als der Beitrag von $\mathfrak{p}$ zur Determinante $\left|\frac{d^{\varkappa}y_i}{dp^{\varkappa}}\right| = \mathfrak{d}_{\mathfrak{p}}(\mathfrak{M})$. Dieser letztere Beitrag

[7]) Dieser Abschnitt ist von mir angefügt worden.

kann nach dem oben bewiesenen Satz leicht bestimmt oder wenigstens abgeschätzt werden.

Ist wieder ohne Einschränkung $\mathfrak{p}$ vom ersten Grade, so existiert bekanntlich eine für $\mathfrak{p}$ normierte Basis y_i von $\mathfrak{M}$ derart, daß $\mathfrak{p}$-adische Entwicklungen als

$$y_i = p^{\varrho_i} + \cdots$$

beginnen, mit einem durch $\mathfrak{M}$ eindeutig bestimmten Exponentensystem

$$\varrho_0 < \varrho_1 < \cdots < \varrho_{n-1}\,.$$

Dann ist

$$\frac{d^\varkappa y_i}{dp^\varkappa} = \binom{\varrho_i}{\varkappa} p^{\varrho_i - \varkappa} + \cdots,$$

und somit

$$\left|\frac{d^\varkappa y_i}{dp^\varkappa}\right| = \left|\binom{\varrho_i}{\varkappa}\right| p^{\Sigma\varrho_i - \Sigma\varkappa} + \cdots.$$

Daraus liest man ab:

Satz. *Ist die Zahldeterminante* $\left|\binom{\varrho_i}{\varkappa}\right|$ $(i, \varkappa = 0, 1, \ldots, n-1)$ *aus dem Exponentensystem* ϱ_i *von* $\mathfrak{M}$ *für* $\mathfrak{p}$ *nicht durch Char. k teilbar, so ist* $\mathfrak{d}(\mathfrak{M})$ *genau durch* $\mathfrak{p}^{\sum_{i=0}^{n-1}(\varrho_i - i)}$ *teilbar, sonst durch eine höhere Potenz von* $\mathfrak{p}$.

Für die Zahldeterminante findet man leicht — am einfachsten durch Betrachtung der ϱ_i als Unbestimmte —

$$\left|\binom{\varrho_i}{\varkappa}\right| = \prod_{i>j} \frac{\varrho_i - \varrho_j}{i - j}\,.$$

Sie ist also jedenfalls von Null verschieden, so daß für Char. $k = 0$ der bewiesene Satz den genauen Beitrag von $\mathfrak{p}$ zu $\mathfrak{d}(\mathfrak{M})$ liefert und insbesondere $\mathfrak{d}(\mathfrak{M}) \neq 0$ ergibt.

Eingegangen 19. November 1936.

Zusatz bei der Korrektur.

Von *F. K. Schmidt* in Jena.

Wie ich nunmehr bemerke, kann man mit dem Verfahren der vorstehenden Note leicht eine formale Theorie der höheren Differentialquotienten in ganz beliebigen Körpern bzw. Integritätsbereichen entwickeln. Diese Verallgemeinerung dürfte für die formale Theorie der Differentialgleichungen in beliebigen Körpern von Interesse sein. Ich will sie daher kurz auseinandersetzen. Dabei brauche ich von den bisher in algebraischen Funktionenkörpern aufgestellten Differentiationstheorien nichts vorauszusetzen. Vielmehr lassen sich diese speziellen Ergebnisse aus den allgemeinen Überlegungen leicht

zurückgewinnen, wodurch die Durchsichtigkeit vielleicht noch etwas erhöht wird. So wird z. B. der Übergang von der Differentiation im Großen zur Differentiation im Kleinen, der im obigen Text noch einen besonderen Kunstgriff erforderte, ganz trivial. Vor allem führen aber die neuen Gesichtspunkte zu einer Bestimmung aller in einem algebraischen Funktionenkörper überhaupt möglichen Differentiationsprozesse. Es stellt sich heraus, daß im Falle der Primzahlcharakteristik die bisher konstruierten Differentiationen nach einer Körperfunktion in bestimmtem Sinne die einzigen sind, was offenbar in auffälligem Gegensatz zu den bekannten Verhältnissen im Fall der Charakteristik 0 steht (Existenz abelscher Integrale).

1. Definition der Differentiation. Ich betrachte einen beliebigen Integritätsbereich $\mathfrak{l}$ von der Charakteristik p ($= 0$ oder Primzahl), dessen Elemente Funktionen heißen mögen. Jeder Funktion y aus $\mathfrak{l}$ sei für jede natürliche Zahl ν jeweils eine weitere Funktion $y^{(\nu)}$ aus einem Oberintegritätsbereich $\mathfrak{l}^*(\geqq \mathfrak{l})$ so zugeordnet, daß die aus der Differentialrechnung bekannte

Summenregel $$(y + z)^{(\nu)} = y^{(\nu)} + z^{(\nu)}$$

und die modifizierte

Produktregel $$(yz)^{(\nu)} = y^{(\nu)}z + y^{(\nu-1)}z' + \cdots + y'z^{(\nu-1)} + yz^{(\nu)}$$

gelten. Ich nenne dann diese Zuordnung eine in $\mathfrak{l}$ erklärte *Differentiation* und bezeichne $y^{(\nu)}$ als ν-te Ableitung von y. Eine Funktion c, deren sämtliche Ableitungen $c^{(\nu)}$ für $\nu \geqq 1$ gleich 0 sind, heiße eine *absolute Differentiationskonstante*; verschwinden dagegen nur alle Ableitungen $c^{(\nu)}$ von einer Ordnung $1 \leqq \nu < \varrho$, während $c^{(\varrho)} \neq 0$ ist, so spreche ich von einer *Differentiationskonstanten ϱ-ter Ordnung*. Die absoluten Differentiationskonstanten können dann offenbar auch als Differentiationskonstanten unendlich hoher Ordnung aufgefaßt werden.

Aus der Summen- und Produktregel erkennt man leicht, daß die Differentiationskonstanten von mindestens ϱ-ter Ordnung einen Teilintegritätsbereich von $\mathfrak{l}$ bilden und daß die Funktionen des Primintegritätsbereichs stets absolute Differentiationskonstanten sind. Ist $\mathfrak{l}$ insbesondere ein Körper, so stellen die Differentiationskonstanten einen Unterkörper dar. Auch die Bezeichnung läßt sich mit Hilfe der Summen- und Produktregel unmittelbar rechtfertigen. Die absoluten Differentiationskonstanten c spielen nämlich bei der Bildung beliebig hoher Ableitungen dieselbe Rolle wie die Konstanten in der gewöhnlichen Differentialrechnung,

$$(y + c)^{(\nu)} = y^{(\nu)}, \qquad (cy)^{(\nu)} = cy^{(\nu)},$$

während die Differentiationskonstanten ϱ-ter Ordnung nur bei den Ableitungen von der Ordnung $\nu < \varrho$ als Konstanten behandelt werden dürfen.

2. Iterative Differentiation. Eine besondere Bedeutung kommt denjenigen Differentiationen zu, bei denen die Ableitungen $y^{(\nu)}$ für alle Funktionen y im ursprünglichen Integritätsbereich $\mathfrak{l}$ liegen, so daß also $\mathfrak{l}^* = \mathfrak{l}$ gesetzt werden kann. Dann können die Ableitungen offenbar wieder differenziert werden und man kann nach der Beziehung der so gewonnenen iterierten Ableitungen $(y^{(\mu)})^{(\lambda)}$ zu den Ableitungen $y^{(\nu)}$ fragen. Ich nenne die gegebene Differentiation insbesondere *iterativ*, wenn für diese iterierten Ableitungen die modifizierte

Iterationsregel $$\binom{\nu}{\mu} y^{(\nu)} = (y^{(\mu)})^{(\nu-\mu)} \qquad (\mu < \nu)$$

gilt. Im Fall der Charakteristik 0 ist die Iterationsregel gleichwertig mit der Gleichung

$$y^{(\nu)} = \frac{(\ldots(y')'\ldots)'}{\nu!}, \tag{1}$$

die die ν-te Ableitung auf die ν-mal iterierte erste Ableitung zurückführt. Im Fall der

Charakteristik $p \neq 0$ zieht dagegen die Iterationsregel die Gleichung (1) nur für $\nu < p$ nach sich, während aus ihr für $\nu \geqq p$ neue Beziehungen fließen, z. B.

$$(y^{(\mu)})^{(\nu-\mu)} = 0\,, \tag{2}$$

wenn ν durch eine höhere Potenz von p teilbar ist als μ.

Für die Differentiationskonstanten besagt die Iterationsregel: Im Fall der Charakteristik 0 ist eine Funktion schon dann absolute Differentiationskonstante, wenn ihre erste Ableitung verschwindet (Beweis durch (1)). Es gibt daher nur Differentiationskonstanten von der Ordnung ∞. — Im Fall der Charakteristik $p \neq 0$ folgt aus $y^{(\mu)} = 0$ die Gleichung $y^{(\nu)} = 0$ für jedes ν, dessen p-adische Koeffizienten nicht kleiner als die von μ sind. (Beweis aus der Iterationsregel, weil unter den angegebenen Voraussetzungen der Binomialkoeffizient $\binom{\nu}{\mu}$ durch p unteilbar ist). Als Ordnungen der Differentiationskonstanten können also außer ∞ nur Potenzen der Charakteristik auftreten.

3. Fragestellungen. Eine beliebige Differentiation braucht, wie sich herausstellen wird, keineswegs iterativ zu sein. Der Integritätsbereich $\mathfrak{l}$ braucht auch selbstverständlich keine Funktion x zu enthalten, für die $x' = 1$ und $x^{(\nu)} = 0$ im Falle $\nu > 1$ ist, d. h. die gegebene Differentiation braucht sich nicht als Differentiation nach einer Funktion des Integritätsbereichs auffassen zu lassen. Trotzdem kann die Theorie beliebiger Differentiationen leicht entwickelt werden.

Dabei interessieren vor allem folgende Aufgaben:

a) Man konstruiere zu einer gegebenen Differentiation des Integritätsbereichs $\mathfrak{l}$ eine zweite, die sich als Differentiation nach einer Funktion von $\mathfrak{l}$ auffassen läßt und aus der die ursprüngliche Differentiation mit Hilfe der „Kettenregel“ zurückgewonnen werden kann.

b) Man bestimme alle Fortsetzungen der gegebenen Differentiation vom Integritätsbereich $\mathfrak{l}$ auf den Quotientenkörper, ferner vom Körper K auf eine einfache transzendente Erweiterung $\mathsf{K}(x)$ und endlich von K auf eine separabel algebraische Erweiterung $\mathsf{K}(w)$. In sämtlichen Fällen untersuche man die Fortpflanzung der Iterationsregel.

c) Man ordne den Fall eines algebraischen Funktionenkörpers in die allgemeine Theorie ein. Insbesondere ermittle man alle iterativen Differentiationen eines algebraischen Funktionenkörpers, bei denen die Elemente des Konstantenkörpers absolute Differentiationskonstanten sind.

Diese Aufgaben sollen im folgenden kurz gelöst werden. Die Lösung von b) ermöglicht es selbstverständlich, auch alle Fortsetzungen einer gegebenen Differentiation auf eine beliebige, separabel erzeugbare Erweiterung anzugeben.

4. Allgemeine Taylorentwicklung. Das wesentliche Hilfsmittel der folgenden Überlegungen besteht darin, daß ich jeder Funktion mit Hilfe der gegebenen Differentiation eine allgemeine Taylorentwicklung zuordne. Das ist nur teilweise neu, denn den Zusammenhang zwischen Differentiation und Taylorentwicklung hat schon H. Hasse benutzt. Er wendet ihn aber entsprechend der üblichen Auffassung der Taylorschen Reihe im Kleinen an, während ich gewissermaßen die Taylorentwicklung für eine „allgemeine“ Stelle hinschreibe. Dadurch wird es möglich, die Taylorentwicklung auch für die Theorie im Großen zu verwerten und die Differentiationstheorie auf die bekannte Theorie der Isomorphismen zwischen Integritätsbereichen bzw. Körpern zurückzuführen, sie also völlig zu trivialisieren.

Ich bilde über $\mathfrak{l}^*$ den Integritätsbereich $\mathfrak{T}^* = \mathfrak{l}^*\{u\}$ aller Potenzreihen in u mit Koeffizienten aus $\mathfrak{l}^*$. Unter der Voraussetzung, daß in $\mathfrak{l}$ eine Differentiation gegeben

sei, bei der die Ableitungen in $\mathfrak{l}^*$ liegen, ordne ich jeder Funktion y von $\mathfrak{l}$ eine eindeutig bestimmte Potenzreihe aus T^* zu,

$$y \to Y = y + y'u + y''u^2 + \cdots + y^{(\nu)}u^\nu + \cdots.$$

Y heiße die allgemeine *Taylorentwicklung* von y bei der gegebenen Differentiation (genauer: u-Taylorenentwicklung $Y = Y_u$). Ihr Anfangsglied ist die Funktion y selbst, so daß also die Funktion umgekehrt durch ihre Taylorentwicklung eindeutig festgelegt ist.

Satz 1. *Ordnet man jeder Funktion y von $\mathfrak{l}$ mit Hilfe der gegebenen Differentiation ihre allgemeine Taylorentwicklung zu, so erhält man einen Isomorphismus von $\mathfrak{l}$ auf einen Teilintegritätsbereich T von T^*.*

Beweis folgt unmittelbar aus der Summen- und Produktregel für die Ableitungen.

Entscheidend ist nun, daß Satz 1 sich umkehren läßt. Ich setze also jetzt nichts über die Differenzierbarkeit der Funktionen von $\mathfrak{l}$ voraus, vielmehr will ich eine Differentiation in $\mathfrak{l}$ erst konstruieren.

Satz 2. *Liegt ein Isomorphismus von $\mathfrak{l}$ auf einen Teilintegritätsbereich von T^* vor, bei dem jeder Funktion y eine Potenzreihe Y aus T^* mit dem Anfangsglied y entspricht, so kann ich die Koeffizienten der Reihe Y als Ableitungen von y auffassen und erhalte dadurch eine Differentiation in $\mathfrak{l}$, bei der die Ableitungen in $\mathfrak{l}^*$ liegen.*

Die Koeffizienten der zugeordneten Reihen genügen nämlich infolge des vorausgesetzten Isomorphismus der Summen- und Produktregel, womit der Beweis bereits erbracht ist.

Satz 1 und 2 besagen zusammengenommen, daß die Theorie der Differentiationen in $\mathfrak{l}$ völlig gleichwertig ist der Theorie der Isomorphismen von $\mathfrak{l}$ auf Potenzreihenintegritätsbereiche, bei denen einer Funktion y jeweils eine Potenzreihe mit dem Anfangsglied y entspricht.

Ich nehme nun an, es liege in $\mathfrak{l}$ eine iterative Differentiation vor. Wie drückt sich dann die Iterationsregel mit Hilfe der allgemeinen Taylorentwicklungen aus? Um das einzusehen, schreibe ich neben der Taylorentwicklung Y von y noch die Taylorentwicklung $Y^{(\mu)}$ der μ-ten Ableitung $y^{(\mu)}$ von y hin,

$$Y^{(\mu)} = y^{(\mu)} + (y^{(\mu)})'u + (y^{(\mu)})''u^2 + \cdots + (y^{(\mu)})^{(\nu-\mu)}\, u^{\nu-\mu} + \cdots.$$

Andererseits denke ich mir in der Potenzreihe Y jeweils die Potenz u^ν durch

$$D_u^\mu u^\nu = \binom{\nu}{\mu} u^{\nu-\mu}$$

ersetzt und erhalte so die Reihe

$$D_u^\mu Y = \binom{\mu}{\mu} y^{(\mu)} + \binom{\mu+1}{\mu} y^{(\mu+1)}u + \cdots + \binom{\nu}{\mu} y^{(\nu)}u^{\nu-\mu} + \cdots.$$

Dann gilt offenbar:

Satz 3. *Die Iterationsregel ist gleichwertig mit der Gültigkeit der Gleichung*

$$Y^{(\mu)} = D_u^\mu Y$$

für sämtliche Taylorentwicklungen Y und alle natürlichen Zahlen μ.

Für die Anwendungen ist es zweckmäßig, Satz 3 noch etwas anders zu deuten. Denkt man sich der Taylorentwicklung Y einer beliebigen Funktion y für jedes μ jeweils die Taylorentwicklung $Y^{(\mu)}$ von $y^{(\mu)}$ zugeordnet,

$$Y \to Y^{(\mu)}, \tag{3}$$

so erhält man wegen des Isomorphismus zwischen $\mathfrak{l}$ und T offenbar eine Differentiation innerhalb des Bereichs T der Taylorentwicklungen. Andererseits stellt aber auch die

Zuordnung

$$Y \to D_u^\mu Y \tag{4}$$

eine Differentiation in T dar, wie man leicht durch Nachrechnen der Summen- und Produktregel bestätigt. Nach Satz 3 ist also die Iterationsregel gleichwertig damit, daß in T die Differentiationen (3) und (4) übereinstimmen.

Aus den vorstehenden Sätzen folgt insbesondere:

Ist in dem Integritätsbereich l *von der Charakteristik* $p \neq 0$ *eine iterative Differentiation gegeben, bei der nicht alle Funktionen aus* l *absolute Differentiationskonstanten sind, aber doch keine Funktion eine von* 0 *verschiedene erste Ableitung besitzt, so erhält man in* l *durch Umnumerierung der Ableitungen eine neue iterative Differentiation, bei der nun mindestens eine Funktion eine nichtverschwindende erste Ableitung hat.*

Aus den Voraussetzungen entnimmt man nämlich nach Nr. **2** (Schluß) die Existenz einer Potenz p^σ der Art, daß

$$y^{(\nu)} = 0 \text{ für alle } y \text{ aus } \mathfrak{l} \text{ und alle } \nu \not\equiv 0 \bmod p^\sigma$$

gilt, während für mindestens eine Funktion x

$$x^{(p^\sigma)} \neq 0$$

ist. Die Taylorentwicklung Y_u einer beliebigen Funktion y ist daher eine Potenzreihe in u^{p^σ},

$$Y_u = y + y^{(p^\sigma)} u^{p^\sigma} + \cdots + y^{(\lambda p^\sigma)} u^{\lambda p^\sigma} + \cdots .$$

Setzt man in ihr $u^{p^\sigma} = v$, so erhält man einen Isomorphismus zwischen den y und Potenzreihen in v,

$$y \to Y_v = y + y^{(p^\sigma)} v + \cdots + y^{(\lambda p^\sigma)} v^\lambda + \cdots ,$$

der offenbar eine neue durch Punkte angedeutete Differentiation

$$\dot{y}^{(\lambda)} = y^{(\lambda p^\sigma)}$$

definiert. Dabei ist $\dot{x} \neq 0$. Da in einem Körper der Charakteristik p stets $\binom{\nu p}{\mu p} = \binom{\nu}{\mu}$ ist, zieht die Iterationsregel für die ursprüngliche Differentiation unmittelbar wieder die Gültigkeit der Iterationsregel für die neue Differentiation nach sich.

Man darf also auch im Fall der Charakteristik $p \neq 0$ von einer iterativen Differentiation, bei der nicht alle Funktionen aus l absolute Differentiationskonstanten sind, ohne Beschränkung der Allgemeinheit voraussetzen, daß schon mindestens eine erste Ableitung nicht verschwindet.

5. Kettenregel. Ich nehme an, in l seien zwei Differentiationen gegeben, eine „gestrichene" Differentiation

$$y', y'', \ldots, y'^{(\nu)}, \ldots$$

und eine „punktierte" Differentiation

$$\dot{y}, \ddot{y}, \ldots, \dot{y}^{(\nu)}, \ldots,$$

bei denen die Ableitungen jeweils in l* liegen. Ich sage dann, die gestrichene Differentiation *gehe mit Hilfe der Funktion* x *aus der punktierten nach der Kettenregel hervor*, wenn man die gestrichene u-Taylorentwicklung einer beliebigen Funktion y,

$$y \to y + y'u + y''u^2 + y'''u^3 + \cdots , \tag{5}$$

mit Hilfe der gestrichenen u-Taylorentwicklung von x,

$$x \to x + x'u + x''u^2 + x'''u^3 + \cdots ,$$

folgendermaßen erhält: Man schreibe die punktierte v-Taylorentwicklung von y hin,

$$y \to y + \dot{y}v + \ddot{y}v^2 + \dddot{y}v^3 + \cdots , \tag{6}$$

und ersetze in ihr überall v durch die Reihe

$$v = x'u + x''u^2 + x'''x^3 + \cdots. \tag{7}$$

In der Tat bestehen dann für die Ableitungen Gleichungen von der Form

$$y'^{(\nu)} = \dot{y}^{(\nu)} g_1 + \dot{y}^{(\nu-1)} g_2 + \cdots + \dot{y} g_\nu,$$

wo $g_1 = (x')^\nu$ und allgemein g_λ ein ganzzahliges Polynom in $x', \ldots, x'^{(\lambda)}$ ist. Diese Gleichungen werden aber üblicherweise gerade als die Kettenregel bezeichnet.

Nunmehr lasse ich die Voraussetzung, daß in $\mathfrak{l}$ noch eine zweite Differentiation gegeben sei, wieder fallen. Ich will vielmehr zu der ursprünglichen gestrichenen Differentiation eine zweite punktierte so konstruieren, daß die gestrichene aus ihr nach der Kettenregel hervorgeht.

Satz 4. *Ist $x' \neq 0$, so gibt es in $\mathfrak{l}$ genau eine neue punktierte Differentiation, aus der die gestrichene mit Hilfe von x nach der Kettenregel hervorgeht. Bei ihr ist $\dot{x} = 1$ und $\dot{x}^{(\nu)} = 0$ für $\nu > 1$. Eine gestrichene Differentiationskonstante der Ordnung ϱ ist auch punktierte Differentiationskonstante der Ordnung ϱ.*

Man kann also die neue punktierte Differentiation als eine Differentiation nach x auffassen. Dementsprechend setze ich $\dot{y}^{(\nu)} = {}'D_x^\nu y$ und nenne ${}'D_x^\nu$ die *zu der gestrichenen Differentiation gehörige Differentiation nach x.*

Der Beweis des Satzes 4 liegt auf der Hand, wenn man die angeführte Definition für die Kettenregel beachtet. Wegen $x' \neq 0$ läßt sich nämlich die aus der gestrichenen Taylorentwicklung von x hervorgehende Reihe (7) umkehren

$$u = x_1 v + x_2 v^2 + x_3 v^3 + \cdots. \tag{8}$$

Die gestrichene Differentiation geht daher aus der punktierten dann und nur dann mit Hilfe von x nach der Kettenregel hervor, wenn die punktierte v-Taylorentwicklung (6) einer beliebigen Funktion y aus der gestrichenen u-Taylorentwicklung (5) dadurch entsteht, daß man u durch (8) ersetzt. Man hat also nur noch zu prüfen, ob die Zuordnung

$$y \to Y_v,$$

die aus (5) durch die Substitution (8) gewonnen wird, auch wirklich wieder einen Isomorphismus darstellt. Das ist aber klar, denn (5) ist nach Voraussetzung ein Isomorphismus und der durch die umkehrbar eindeutige Substitution (8) bewirkte Übergang

$$y + y'u + y''u^2 + y'''u^3 + \cdots \to Y_v$$

ist sicher ebenfalls ein Isomorphismus.

Da (8) Umkehrung von (7) ist, ergibt sich schließlich aus der gestrichenen u-Taylorentwicklung von x durch die Substitution (8) die Reihenentwicklung

$$X_v = x + v,$$

d. h. $\dot{x} = 1, \dot{x}^{(\nu)} = 0$ für $\nu > 1$. Ebenso leicht erhält man die Behauptung über die Differentiationskonstanten.

6. Fortsetzung einer beliebigen Differentiation. Die Aufgabe, eine in $\mathfrak{l}$ gegebene Differentiation auf einen Oberintegritätsbereich fortzusetzen, ist nach Nr. 4 gleichwertig mit der Aufgabe, den Isomorphismus von $\mathfrak{l}$, der durch Zuordnung der allgemeinen Taylorentwicklungen entsteht, so fortzusetzen, daß wieder jeder Funktion eine Potenzreihe mit der Funktion selbst als Anfangsglied entspricht. Ohne Beschränkung der Allgemeinheit kann und soll dabei vorausgesetzt werden, daß der Integritätsbereich $\mathfrak{l}^*$, der die Ableitungen der Funktionen aus $\mathfrak{l}$ enthält, auch den Oberintegritätsbereich umfaßt, auf den die Differentiation fortgesetzt wird, denn nötigenfalls kann man ja $\mathfrak{l}^*$ beliebig vergrößern.

Satz 5. *Eine im Integritätsbereich* $\mathfrak{l}$ *gegebene Differentiation läßt sich nur auf eine Weise auf den Quotientenkörper* $Q(\mathfrak{l})$ *fortsetzen. Die Ableitungen der Funktionen von* $Q(\mathfrak{l})$ *liegen wieder in* $\mathfrak{l}^*(\geqq Q(\mathfrak{l}))$.

Ist die Differentiation in $\mathfrak{l}$ *iterativ, so pflanzt sich auch die Iterationsregel fort.*

In der Tat, der Isomorphismus von $\mathfrak{l}$ auf den Bereich T der Taylorentwicklungen, der entsteht, wenn man jeder Funktion mit Hilfe der gegebenen Differentiation ihre allgemeine Taylorentwicklung zuordnet, läßt sich auf eine und nur eine Weise zu einem Isomorphismus von $Q(\mathfrak{l})$ fortsetzen. Dabei entspricht jedem Quotienten zweier Funktionen aus $\mathfrak{l}$ der Quotient ihrer Taylorentwicklungen, also eine Potenzreihe, die jedenfalls mit dem betreffenden Funktionsquotienten als Anfangsglied beginnt und lauter Koeffizienten aus $\mathfrak{l}^*$ besitzt. Damit ist der erste Teil des Satzes 5 bereits bewiesen, und zwar habe ich durch die Fortsetzung einen Isomorphismus zwischen $Q(\mathfrak{l})$ und $Q(\mathsf{T})$ erhalten.

Ich nehme nun an, die in $\mathfrak{l}$ gegebene Differentiation sei iterativ. Dann liegen die Ableitungen der Funktionen von $\mathfrak{l}$ jedenfalls in $\mathfrak{l}$. Man kann also $\mathfrak{l}^* = Q(\mathfrak{l})$ wählen und erkennt zunächst, daß bei der Fortsetzung der Differentiation die Ableitungen der Funktionen von $Q(\mathfrak{l})$ wieder zu $Q(\mathfrak{l})$ gehören.

Bei der Fortsetzung der Differentiation besitzt also nicht nur jede Funktion y eine Taylorentwicklung Y in $Q(\mathsf{T})$, sondern auch jede Ableitung $y^{(\mu)}$ von y hat in $Q(\mathsf{T})$ ihre Taylorentwicklung $Y^{(\mu)}$. Wie schon in Nr. **4** erwähnt, stellt die Zuordnung

$$Y \to Y^{(\mu)} \tag{3}$$

eine Differentiation in $Q(\mathsf{T})$ dar. Ebenso ist auch die Zuordnung

$$Y \to D_u^{\mu} Y \tag{4}$$

eine Differentiation in $Q(\mathsf{T})$. Da in $\mathfrak{l}$ die Iterationsregel gilt, stimmen die Differentiationen (3) und (4) nach Satz 3 im Integritätsbereich T überein. Wegen der bereits bewiesenen Eindeutigkeit der Fortsetzung einer Differentiation auf den Quotientenkörper müssen sie dann aber auch für den Quotientenkörper $Q(\mathsf{T})$ von T identisch sein, d. h. auch in $Q(\mathsf{T})$ gilt nach Satz 3 die Iterationsregel.

Satz 6. *Eine in einem Körper* K *gegebene Differentiation läßt sich auf eine und nur eine Weise auf eine einfache transzendente Erweiterung* $\mathsf{K}(x)$ *so fortsetzen, daß die Ableitungen von* x *gleich beliebig vorgegebenen Funktionen aus* $\mathfrak{l}^*$ $(\geqq \mathsf{K}(x))$ *werden. Die Ableitungen der Funktionen von* $\mathsf{K}(x)$ *liegen wieder in* $\mathfrak{l}^*$.

Ist die Differentiation in K *iterativ und genügen auch die gegebenen Ableitungen von* x *der Iterationsregel, so pflanzt sich die Iterationsregel auf* $\mathsf{K}(x)$ *fort.*

Zum Beweis betrachte ich den Isomorphismus zwischen K und T, der entsteht, wenn man jeder Funktion z aus K mit Hilfe der gegebenen Differentiation ihre Taylorentwicklung zuordnet

$$z \to Z\,. \tag{9}$$

Außerdem schreibe ich die Taylorentwicklung X von x bei den vorgegebenen Ableitungen $x^{(\nu)}$ hin

$$X = x + x'u + x''u^2 + \cdots + x^{(\nu)}u^{\nu} + \cdots\,. \tag{10}$$

Die Potenzreihe X ist transzendent in bezug auf den Integritätsbereich T der Taylorentwicklungen Z, weil ihr Anfangsglied x nach Voraussetzung transzendent in bezug auf die Menge der Anfangsglieder aller Z ist. Fügt man daher zu dem Isomorphismus (9) noch die Zuordnung (10) hinzu, so erhält man eine Fortsetzung des Isomorphismus auf $\mathsf{K}(x)$, bei der offenbar jeder Funktion von $\mathsf{K}(x)$ eine Reihe mit der Funktion selbst als Anfangsglied und mit lauter Koeffizienten aus $\mathfrak{l}^*$ entspricht. Diese Fortsetzung ist

aber auch die einzige, bei der x die vorgeschriebene Taylorentwicklung besitzt. Damit ist der erste Teil des Satzes 6 schon bewiesen.

Der zweite ergibt sich wieder leicht mit Hilfe von Satz 3 aus der soeben bestätigten Eindeutigkeitsaussage. Ich nehme also jetzt an, die in K gegebene Differention sei iterativ und die Ableitungen von x genügen ebenfalls der Iterationsregel. Da man nun $\mathsf{l}^* = \mathsf{K}(x)$ wählen kann, liegen die Ableitungen bei der Fortsetzung der gegebenen Differentiation zunächst sicher in $\mathsf{K}(x)$.

Für den $\mathsf{K}(x)$ entsprechenden Körper $\mathsf{T}(X)$ der Taylorentwicklungen läßt sich daher wieder auf zwei Weisen eine Differentiation erklären. Einmal, indem man der Taylorentwicklung Y einer beliebigen Funktion y für jedes $\mu \geqq 1$ die Taylorentwicklung $Y^{(\mu)}$ der Ableitung $y^{(\mu)}$ zuordnet,

$$Y \to Y^{(\mu)}, \tag{3}$$

andererseits, indem man zu Y die Reihe $D_u^\mu Y$ bildet,

$$Y \to D_u^\mu Y\,. \tag{4}$$

Beide Differentiationen stimmen unter den jetzigen Voraussetzungen nach Satz 3 im Körper T und für X überein. Da aber eine Differentiation einer einfachen transzendenten Erweiterung, wie soeben gezeigt wurde, durch die Differentiation im Grundkörper und die Ableitungen des adjungierten transzendenten Elements eindeutig bestimmt ist, müssen die Differentiation (3) und (4) notwendig im ganzen Körper $\mathsf{T}(X)$ übereinstimmen, d. h. in $\mathsf{K}(x)$ gilt wieder die Iterationsregel.

Selbstverständlich ist es leicht, für die Transzendente x Ableitungen anzugeben, die der Iterationsregel genügen. Man setze etwa

$$x' = 1, \quad x^{(\nu)} = 0 \text{ für } \nu > 1\,.$$

Satz 7. *Eine im Körper* K *gegebene Differentiation läßt sich auf eine und nur eine Weise auf eine separabel algebraische Erweiterung* $\mathsf{K}(w)$ *fortsetzen. Die Ableitungen der Funktionen von* $\mathsf{K}(w)$ *liegen wieder in* l^* $(\geqq \mathsf{K}(w))$.

Ist die Differentiation in K *iterativ, so pflanzt sich auch die Iterationsregel fort.*

Es handelt sich wieder darum, den Isomorphismus

$$z \to Z \tag{9}$$

zwischen den Funktionen aus K und ihren Taylorentwicklungen so auf $\mathsf{K}(w)$ fortzusetzen, daß jeder Funktion aus $\mathsf{K}(w)$ eine Potenzreihe mit der Funktion selbst als Anfangsglied entspricht. Dazu betrachte ich das irreduzible Polynom

$$g(t) = t^n + z_1 t^{n-1} + \cdots + z_n$$

über K, das für $t = w$ verschwindet, und ersetze in ihm die Koeffizienten z_i durch ihre Taylorentwicklungen Z_i, so daß ein Polynom

$$G(t) = t^n + Z_1 t^{n-1} + \cdots + Z_n$$

über dem Bereich T der Taylorentwicklungen entsteht. Bekanntlich erhält man alle Fortsetzungen des Isomorphismus (9) auf $\mathsf{K}(w)$, indem man w der Reihe nach die verschiedenen Nullstellen von $G(t)$ zuordnet. Satz 7 ist daher bewiesen, wenn ich zeige, daß $G(t)$ in dem Potenzreihenbereich $\mathsf{l}^*\{u\}$ genau eine Nullstelle mit dem Anfangsglied w besitzt, wie groß ich auch l^* wählen mag.

Diese letzte Behauptung folgt aber unmittelbar aus dem Henselschen Lemma, indem ich $G(t)$ modulo der Unbestimmten u betrachte, nach der die Potenzreihen aus $\mathsf{l}^*\{u\}$ fortschreiten. Offenbar ist nämlich

$$G(t) \equiv g(t) \mod u\,,$$

und da $g(t)$ nach Voraussetzung in $\mathfrak{l}^*(\geqq \mathfrak{l})$ die einfache Nullstelle w besitzt, wird $G(t)$ tatsächlich nach dem Henselschen Lemma durch genau eine Potenzreihe aus $\mathfrak{l}^*\{u\}$ mit dem Anfangsglied w annulliert.

Der zweite Teil des Satzes 7 kann nun wieder mit Hilfe von Satz 3 aus der soeben bestätigten Eindeutigkeitsaussage gewonnen werden. Da der Gedankengang ganz entsprechend verläuft wie bei den Sätzen 5 und 6, führe ich ihn nicht wieder durch.

Zusatz. *Ist w bereits über dem Unterkörper K_ϱ der Differentiationskonstanten von mindestens ϱ-ter Ordnung separabel algebraisch, so ist w selbst eine Differentiationskonstante von mindestens ϱ-ter Ordnung.*

Folgerung. *Mit Hilfe der Sätze 6 und 7 lassen sich alle Fortsetzungen einer im Körper K gegebenen Differentiation auf eine beliebige separabel erzeugbare Erweiterung Λ konstruieren.*

7. Einordnung der algebraischen Funktionenkörper. Gegeben sei nunmehr ein Körper K algebraischer Funktionen in einer Unbestimmten mit dem Konstantenkörper k. K sei separabel erzeugbar. Auf Grund der vorhergehenden Sätze kann ich dann alle Differentiationen von K konstruieren, bei denen die Elemente des Konstantenkörpers absolute Differentiationskonstanten sind. Die Forderung, daß jedes c aus k absolute Differentiationskonstante ist, besagt nämlich, daß ich in k die iterative Differentiation

$$c^{(\nu)} = 0$$

für alle c aus k und alle $\nu \geqq 1$ als gegeben ansehe. Ihre sämtlichen Fortsetzungen auf den separabel erzeugbaren Oberkörper K kann ich aber nach Satz 6 und 7 tatsächlich bilden. In dieser Nummer will ich aus den so entstehenden Differentiationen gewisse iterative Differentiationen nach Körperfunktionen hervorheben und ihre Eigenschaften zusammenstellen.

Ist x eine separierende Funktion von K/k, so gibt es nach Satz 6 eine eindeutig bestimmte iterative Differentiation von $k(x)$, bei der die Elemente von k absolute Differentiationskonstanten sind und x die Ableitungen $x' = 1$, $x^{(\nu)} = 0$ für $\nu > 1$ hat. Diese Differentiation läßt sich eindeutig auf die separabel algebraische Erweiterung K von $k(x)$ fortsetzen. Die so definierte Differentiation, die sich offenbar als Differentiation nach x auffassen läßt, will ich mit D_x^ν bezeichnen und sie kurz *Differentiation nach x* nennen. Sie ist iterativ und ist bereits eindeutig bestimmt durch die Forderungen

$$D_x^\nu c = 0 \text{ für jedes } c \text{ aus } k \text{ und jedes } \nu \geqq 1,$$
$$D_x^1 x = 1,\ D_x^\nu x = 0 \text{ für } \nu > 1.$$

Für ein Polynom

$$a = \sum_{\mu=0}^{n} c_\mu x^\mu$$

aus $k[x]$ folgt daraus mit Hilfe der Summen- und Produktregel unmittelbar

$$D_x^\nu a = \sum_{\mu=0}^{n} \binom{\mu}{\nu} c_\mu x^{\mu-\nu}.$$

Für eine beliebige Funktion y aus K läßt sich wenigstens noch die erste Ableitung leicht explizit hinschreiben. Ist nämlich

$$\Sigma\, c_{\lambda\mu} x^\lambda y^\mu = 0 \tag{10}$$

die irreduzible Gleichung zwischen x und y über k, so ergibt die Summen- und Produktregel

$$\Sigma\, \lambda c_{\lambda\mu} x^{\lambda-1} y^\mu + D_x^1 y\, \Sigma_\mu c_\lambda x^\lambda y^{\mu-1} = 0$$

oder

$$D_x^1 y = -\frac{\sum \lambda c_{\lambda\mu} x^{\lambda-1} y^\mu}{\sum \mu c_{\lambda\mu} x^\lambda y^{\mu-1}}.$$

Ist also y ebenfalls separierend, so daß in (10) mindestens eine Potenz von x mit einem durch die Charakteristik unteilbaren Exponenten λ auftritt, so ist ersichtlich $D_x^1 y \neq 0$.

Ich denke mir nun den Körper K so in einen Potenzreihenkörper $\bar{k}\{x\}$ von Potenzreihen nach x mit Koeffizienten aus einem Oberkörper $\bar{k}$ von k eingebettet, daß das Polynom

$$\sum_{\mu=0}^{n} c_\mu x^\mu \qquad (c_\mu \text{ aus } k)$$

des Körpers K jeweils mit der abbrechenden Potenzreihe

$$\sum_{\mu=0}^{n} c_\mu x^\mu$$

des Potenzreihenkörpers $\bar{k}\{x\}$ identifiziert ist. Jeder Funktion y aus K entspricht bei der Einbettung eindeutig eine Potenzreihe des Körpers $\bar{k}\{x\}$, die ich als Potenzreihenentwicklung von y nach x auffasse. Es handelt sich dann darum, aus der Potenzreihenentwicklung von y die Potenzreihenentwicklung der ν-ten Ableitung $D_x^\nu y$ abzulesen.

Ist

$$y = \sum_{\mu=\mu_0}^{\infty} c_\mu x^\mu,$$

so ist

$$D_x^\nu y = \sum_{\mu=\mu_0}^{\infty} \binom{\mu}{\nu} c_\mu x^{\mu-\nu}.$$

In der Tat, die Zuordnung

$$\sum_{\mu=\mu_0}^{\infty} c_\mu x^\mu \to \sum_{\mu=\mu_0}^{\infty} \binom{\mu}{\nu} c_\mu x^{\mu-\nu} \tag{11}$$

stellt eine Differentiation in $\bar{k}\{x\}$ dar, die für den Polynombereich $k[x]$ mit der in K erklärten Differentiation nach x übereinstimmt. Daraus folgt aber sofort, daß die Zuordnung (11) notwendig für den ganzen Unterkörper K von $k\{x\}$ mit der in K erklärten Differentiation nach x übereinstimmt, denn diese Differentiation ist durch $D_x^\nu c = 0$ für jedes c aus k und jedes ν, $D_x^1 x = 1$, $D_x^\nu x = 0$ für $\nu > 1$ eindeutig bestimmt. Es ist daher wirklich

$$D_x^\nu y = \sum_{\mu=\mu_0}^{\infty} \binom{\mu}{\nu} c_\mu x^{\mu-\nu}.$$

8. Bestimmung aller iterativen Differentiationen des algebraischen Funktionenkörpers *K*. In dem separabel erzeugbaren algebraischen Funktionenkörper K sei eine beliebige iterative Differentiation gegeben, bei der die Elemente des Konstantenkörpers k absolute Differentiationskonstanten sind. Die Ableitungen einer beliebigen Funktion y bei dieser Differentiation werden durch

$$y', y'', \ldots, y^{(\nu)}, \ldots$$

gekennzeichnet. Selbstverständlich schließe ich den trivialen Fall aus, daß überhaupt alle Funktionen aus K bei der gegebenen Differentiation absolute Differentiationskonstanten sind und kann dann nach Nr. **4** ohne Beschränkung der Allgemeinheit annehmen, daß mindestens eine Funktion x aus K eine nichtverschwindende erste Ableitung $x' \neq 0$ besitzt. Daran halte ich im folgenden stets fest.

Satz 8. *Jede Funktion x, deren erste Ableitung $x' \neq 0$ ist, ist separierend.*

Diese Behauptung bedarf natürlich nur im Falle $p \neq 0$ eines Beweises.

Nach Voraussetzung enthält K eine separierende Funktion t. x ist selbst separierend, falls t über $k(x)$ separabel algebraisch ist. Angenommen, t sei über $k(x)$ nicht separabel algebraisch, d. h. in der irreduziblen Gleichung

$$\sum c_{\lambda\mu} t^{\lambda} x'^{\mu} = 0$$

mit Koeffizienten aus k, sei jeder wirklich vorkommende Exponent λ durch die Charakteristik p teilbar, während notwendig ein Exponent μ durch p unteilbar ist, weil ja x von der separierenden Funktion t separabel algebraisch abhängt. Es ist dann also x separabel algebraisch über $k(t^p)$. Da aber alle Funktionen aus $k(t^p)$ Differentiationskonstanten von mindestens p-ter Ordnung sind, folgt daraus nach dem Zusatz zu Satz 7 die Gleichung $x' = 0$ entgegen der Annahme.

Satz 9. *Ist $x' \neq 0$, so geht die gegebene gestrichene Differentiation aus der Differentiation D_x^ν mit Hilfe der Funktion x nach der Kettenregel hervor.*

Da $x' \neq 0$ ist, gibt es nämlich nach Satz 4 in K eine eindeutig bestimmte Differentiation ${}'D_x^\nu$, aus der die gestrichene Differentiation mit Hilfe von x nach der Kettenregel hervorgeht. Dabei ist

$${}'D_x^\nu c = 0 \text{ für jedes } c \text{ aus } k \text{ und alle } \nu,$$

weil die c bei der gestrichenen Differentiation absolute Differentiationskonstanten sind; ferner ist

$${}'D_x^1 x = 1, \quad {}'D_x^\nu x = 0 \quad \text{für } \nu > 1.$$

Durch diese Gleichungen ist aber gerade die Differentiation D_x^ν gekennzeichnet. Es ist daher ${}'D_x^\nu = D_x^\nu$, d. h. die gestrichene Differentiation geht tatsächlich aus D_x^ν mit Hilfe von x nach der Kettenregel hervor.

Folgerung. *Sind x und y zwei separierende Funktionen von K, so geht die Differentiation D_y^ν aus der Differentiation D_x^ν mit Hilfe von x nach der Kettenregel hervor.*

Für die separierende Funktion x ist nämlich $D_y^1 x \neq 0$, so daß man Satz 9 anwenden kann, indem man die dort vorkommende beliebige gestrichene Differentiation mit D_y^ν identifiziert.

Nach diesen Vorbemerkungen bestimme ich nun sämtliche überhaupt möglichen iterativen Differentiationen in K. Im Fall der Charakteristik 0 bietet das Ergebnis nichts Neues. Da es sich mühelos gewinnen läßt, begnüge ich mich damit, es anzugeben: *Ist x eine feste nichtkonstante Funktion von K, so gibt es zu jeder Funktion z von K genau eine Differentiation, bei der die erste Ableitung von x gleich z ist. Durch die so gewonnenen Differentiationen werden alle Differentiationen von K erschöpft.* Unter ihnen befinden sich solche, die sich nicht als Differentiation nach einer Funktion aus K auffassen lassen.

Von besonderem Interesse ist dagegen der Fall der Charakteristik $p \neq 0$. Seine Untersuchung bereite ich durch zwei Sätze vor, die sich auf die Differentiationskonstanten ϱ-ter Ordnung und auf die Integration der Differentialgleichung $y' = z$ innerhalb von K beziehen. Ich denke mir dabei in dem Körper K von Primzahlcharakteristik wieder eine beliebige iterative Differentiation gegeben, bei der die Elemente von k Differentiationskonstanten sind und mindestens ein x eine nichtverschwindende erste Ableitung $x' \neq 0$ besitzt. Sie werde wieder durch Striche gekennzeichnet und die gestrichene Differentiation genannt.

Satz 10. *Der Körper K_σ der Differentiationskonstanten von mindestens p^σ-ter Ordnung bei der gegebenen Differentiation ist gleich kK^{p^σ}, $K_\sigma = kK^{p^\sigma}$.*

Offenbar ist nämlich $K_\sigma \geqq kK^{p^\sigma}$. Andererseits umfaßt ein echter Oberkörper von kK^{p^σ} notwendig den Körper $kK^{p^{\sigma-1}}$, weil $kK^{p^{\sigma-1}}/kK^{p^\sigma}$ vom Grade p ist. Da aber K_σ die zu $kK^{p^{\sigma-1}}$ gehörige Funktion $x^{p^{\sigma-1}}$ sicher nicht enthält, ist tatsächlich $K_\sigma = kK^{p^\sigma}$.

Insbesondere ist also $K_1 = kK^p$. Beachtet man, daß K/kK^p vom Grade p und zwar $K = kK^p(x)$ ist, mithin für jedes z aus K eine Darstellung

$$z = c_0 + c_1 x + \cdots + c_{p-1} x^{p-1} \text{ mit } c_i \text{ aus } kK^p = K_1 \tag{12}$$

besteht, so erhält man zunächst für die Differentiation nach x eine einfache, aber grundlegende Folgerung, auf die schon O. Teichmüller hingewiesen hat.

Folgerung. *K enthält ein Integral y der Differentialgleichung $D_x^1 y = z$, sobald $D_x^{p-1} z = 0$ ist.*

Nach (12) ist nämlich $D_x^{p-1} z = c_{p-1}$. Infolge der Voraussetzung $D_x^{p-1} z = 0$ verschwindet also c_{p-1}. Die Funktion

$$y = c_0 x + \frac{c_1}{2} x^2 + \cdots + \frac{c_{p-2}}{p-1} x^{p-1}$$

genügt daher der Differentialgleichung $D_x^1 y = z$.

Daß die angegebene Bedingung für die Lösbarkeit der Differentialgleichung auch notwendig ist, entnimmt man leicht der Iterationsregel, die $D_x^{p-1}(D_x^1 y) = 0$ ergibt.

Die soeben angegebene Folgerung läßt sich aber sogar auf die beliebig gegebene gestrichene Differentiation ausdehnen.

Satz 11. *K enthält ein Integral y der Differentialgleichung $y' = z$, sobald $z^{(p-1)} = 0$ ist.*

Zum Beweis führe ich an Stelle der gestrichenen Differentiation die Differentiation D_x^ν ein, aus der die gestrichene Differentiation nach Satz 9 mit Hilfe von x nach der Kettenregel hervorgeht. Offenbar ist $D_x^1 y = \frac{y'}{x'}$. Die Lösung der Differentialgleichung $y' = z$ ist daher mit der Auflösung der Differentialgleichung $D_x^1 y = \frac{z}{x'}$ gleichbedeutend. Diese letzte Differentialgleichung besitzt aber nach der soeben angeführten Folgerung in K ein Integral, falls für die Funktion

$$w = \frac{z}{x'}$$

die $(p-1)$-te Ableitung $D_x^{p-1} w = 0$ ist. Ich werde daher $D_x^{p-1} w$ berechnen.

Dabei habe ich lediglich zu beachten, daß die gestrichene Differentiation aus der Differentiation D_x^ν mit Hilfe von x nach der Kettenregel hervorgeht. Die Ableitung $D_x^\nu w$ ist infolgedessen gleich dem Koeffizienten von v^ν in der Potenzreihe nach v, die sich aus der gestrichenen u-Taylorentwicklung von w

$$W = w + w'u + w''u^2 + \cdots$$

ergibt, indem man u durch die Inverse der Reihe

$$v = x'u + x''u^2 + \cdots = X - x$$

ersetzt. Die so entstehenden Koeffizienten können aber durch Übertragung der Bürmann-Lagrangeschen Entwicklung bestimmt werden. Dabei dürfen wir uns noch auf die Koeffizienten der Potenzen v^ν mit $\nu < p$ beschränken, weil uns nur $D_x^{p-1} w$ interessiert, und gerade diese Koeffizienten lassen sich unmittelbar nach dem Vorbild der Funktions-

theorie ermitteln. Da nämlich die Iterationsregel für $\nu < p$ die ν-te Ableitung auf die ν-mal iterierte erste zurückführt, läßt sich für $\nu < p$ der bei Goursat (Cours d'analyse I) wiedergegebene Laplacesche Beweis der Bürmann-Lagrangeschen Entwicklung übertragen und liefert:

$$D_x^{p-1} w = \text{Koeffizient von } u^{p-1} \text{ in } W D_u^1(X) \left(\frac{u}{X-x}\right)^p,$$

wo $D_u^1(X)$ die schon früher eingeführte Ableitung von

$$X = x + x'u + x''u^2 + \cdots$$

nach u bedeutet. Bedenkt man, daß

$$W = \frac{Z}{X'} = \frac{z + z'u + \cdots}{x' + (x')'u + \cdots}$$

der Quotienten der gestrichenen u-Taylorentwicklungen von z und x' ist, und daß infolge der Iterationsregel

$$X' = D_u^1 X$$

gilt, so hat man schließlich

$$D_x^{p-1} w = \text{Koeffizient von } u^{p-1} \text{ in } Z\left(\frac{u}{X-x}\right)^p.$$

Nun ist

$$\left(\frac{u}{X-x}\right)^p \equiv \left(\frac{1}{x'}\right)^p \mod u^p.$$

Ferner ist nach Voraussetzung $z^{(p-1)} = 0$, also

$$Z\left(\frac{u}{X-x}\right)^p \equiv (z + z'u + \cdots + z^{(p-2)}u^{p-2})\left(\frac{1}{x'}\right)^p \mod u^p,$$

d. h. der Koeffizient von u^{p-1} ist 0 und daher wirklich

$$D_x^{p-1} w = 0.$$

Satz 12. *Ist in K eine beliebige iterative Differentiation $y \to y^{(\nu)}$ gegeben, bei der die Elemente aus k absolute Differentiationskonstanten sind, und ist m eine beliebige natürliche Zahl, so gibt es in K stets eine separierende Funktion $t = t_m$ der Art, daß*

$$D_t^\nu y = y^{(\nu)}$$

gilt für alle y aus K und alle $\nu < m$.

Die beliebig vorgegebene iterative Differentiation stimmt also gleichzeitig für alle y aus K hinsichtlich beliebig vieler Ableitungen mit der Differentiation nach einer geeigneten Körperfunktion t überein. Allerdings hängt die Funktion t noch ab von der Anzahl der Ableitungen, deren Übereinstimmung für alle y aus K gefordert wird. Vergrößert man m, so ändert sich im allgemeinen t, und es ist im allgemeinen auch nicht möglich, t so zu bestimmen, daß die Ableitungen jeder Ordnung gleich werden. Trotzdem wird man auf Grund von Satz 12 sagen dürfen, daß die iterativen Differentiationen in K, bei denen die Elemente von k absolute Differentiationskonstanten sind, im wesentlichen durch die in der vorigen Nummer eingeführten Differentiationen nach separierenden Körperfunktionen erschöpft werden. Dabei ist wie immer vorausgesetzt, daß bei der gegebenen Differentiation mindestens eine Funktion eine nichtverschwindende Ableitung besitzt.

Zum Beweis des Satzes 12 genügt es, zu zeigen, daß es in K eine Funktion t gibt, für die $t' = 1$ und $t^{(\nu)} = 0$ im Falle $1 < \nu < m$ ist. Eine solche ist nämlich nach Satz 8 separierend, so daß man die Ableitungen D_t^ν nach der Vorschrift der vorigen Nummer

bilden kann. Die ursprünglich gegebene gestrichene Differentiation geht ferner nach Satz 9 aus der Differentiation D_t^ν mit Hilfe der Funktion t nach der Kettenregel hervor. Man erhält also die gestrichene u-Taylorentwicklung einer beliebigen Funktion y

$$y \to y + y'u + y''u^2 + y'''u^3 + \cdots$$

mit Hilfe der gestrichenen u-Taylorentwicklung von t

$$t \to t + u + t^{(m)}u^m + \cdots,$$

indem man in die v-Taylorentwicklung von y bei der Differentiation D_t^ν

$$y \to y + (D_t^1 y)\, v + (D_t^2 y)\, v^2 + \cdots$$

überall für v die Reihe

$$v = u + t^{(m)}u^m + \cdots$$

einsetzt. Bei dieser Einsetzung ergibt sich aber offenbar

$$y^{(\nu)} = D_t^\nu y \text{ für } \nu < m,$$

d. h. Satz 12 ist tatsächlich bewiesen, sobald in K eine Lösung t des angegebenen Systems von Differentialgleichungen gefunden ist.

Ich betrachte also nunmehr das unendliche System von Differentialgleichungen

$$y' = 1, \quad y^{(\nu)} = 0 \text{ für } \nu > 1. \tag{13}$$

Zu einer beliebig vorgegebenen Potenz p^σ der Charakteristik werde ich durch vollständige Induktion ein in K enthaltenes Integral derjenigen Differentialgleichung (13) konstruieren, für die $\nu \leqq p^\sigma$ ist. Wählt man dann $p^\sigma \geqq m$, so hat man insbesondere ein Integral t der Differentialgleichungen (13) mit $\nu < m$, auf das es mir ankommt.

Der Induktionsbeginn ($\sigma = 0$) ist rasch erledigt. Da nämlich die $(p-1)$-te Ableitung von 1 verschwindet, besitzt die Differentialgleichung $y' = 1$ nach Satz 11 sicher ein Integral in K.

Ich mache jetzt die Induktionsannahme, daß ein in K enthaltenes Integral $y = \eta$ aller Gleichungen (13) mit $\nu \leqq p^{\sigma-1}$ schon konstruiert sei ($\sigma - 1 \geqq 0$). Auf Grund dieser Annahme werde ich die Differentialgleichungen (13) mit $\nu \leqq p^\sigma$ innerhalb des Körpers K lösen.

Die Funktion $y = \eta$ befriedigt ganz von selbst schon alle Differentialgleichungen (13), für die $\nu \not\equiv 0 \bmod. p^\sigma$ ist. Zu jedem solchen ν gibt es nämlich eine nicht negative Zahl $\mu \leqq p^{\sigma-1}$, die durch die gleiche Potenz von p teilbar ist wie ν. Der Binomialkoeffizient $\binom{\nu}{\mu}$ ist dann durch p unteilbar und folglich ist

$$\eta^{(\nu)} = \frac{(\eta^{(\mu)})^{(\nu-\mu)}}{\binom{\nu}{\mu}} = 0 \text{ für } \nu > 1,\ \nu \not\equiv 0 \bmod. p^\sigma,$$

weil ja nach Induktionsannahme $\eta^{(\mu)} = 1$ oder 0 ist. Addiere ich ferner zu η eine beliebige Funktion a des Körpers kK^{p^σ}, so bleibt auch

$$y = \eta + a$$

eine Lösung aller Differentialgleichungen (13) mit $\nu \not\equiv 0 \bmod. p^\sigma$, denn für jedes derartige ν ist $a^{(\nu)} = 0$. Ich werde nun die Funktion a aus kK^{p^σ} so zu bestimmen suchen, daß

$$y = \eta + a$$

auch noch der Differentialgleichung

$$y^{(p^\sigma)} = 0$$

genügt, und habe dann die Induktion beendet. Setzt man $-\eta^{(p^\sigma)} = r$, so ergibt das

offenbar für die Funktion a die beiden Bedingungen

$$a = \text{Funktion aus } kK^{p^\sigma}, \quad a^{(p^\sigma)} = r. \tag{14}$$

Für jede nichtnegative ganze Zahl $\varrho < \sigma$ ist

$$r^{(p^\varrho)} = -\,(\eta^{(p^\sigma)})^{(p^\varrho)} = -\binom{p^\sigma + p^\varrho}{p^\sigma}\eta^{(p^\sigma+p^\varrho)} = 0,$$

weil $p^\sigma + p^\varrho \not\equiv 0 \bmod p^\sigma$ und daher $\eta^{(p^\sigma+p^\varrho)} = 0$ ist. Nach Satz 10 liegt also r in kK^{p^σ}, und zwar kann ich r auf die Gestalt

$$r = r_1^{p^\sigma} c_1 + r_2^{p^\sigma} c_2 + \cdots + r_h^{p^\sigma} c_h$$

bringen, wo die c_i über K^{p^σ} linear unabhängige Elemente aus k seien. Die unbekannte Funktion a aus kK^{p^σ} setze ich dann in der Form

$$a = x_1^{p^\sigma} c_1 + x_2^{p^\sigma} c_2 + \cdots + x_h^{p^\sigma} c_h$$

an und habe hierin die Funktionen x_i so zu wählen, daß

$$a^{(p^\sigma)} = r, \text{ also } (x_1')^{p^\sigma} c_1 + (x_2')^{p^\sigma} c_2 + \cdots + (x_h')^{p^\sigma} c_h = r_1^{p^\sigma} c_1 + r_2^{p^\sigma} c_2 + \cdots + r_h^{p^\sigma} c_h$$

ist. Wegen der linearen Unabhängigkeit der c_i über K^{p^σ} ist die letzte Gleichung gleichbedeutend mit den h Differentialgleichungen

$$x_i' = r_i, \tag{15}$$

deren Lösbarkeit in K ich nun noch mit Hilfe von Satz 11 zu prüfen habe.

Auf Grund der Iterationsregel gilt

$$r^{(p^{\sigma+1}-p^\sigma)} = \left(-\,\eta^{(p^\sigma)}\right)^{(p^{\sigma+1}-p^\sigma)} = -\binom{p^{\sigma+1}}{p^\sigma}\eta^{(p^{\sigma+1})} = 0,$$

weil $\binom{p^{\sigma+1}}{p^\sigma}$ durch p teilbar ist. Andererseits findet man

$$r^{(p^{\sigma+1}-p^\sigma)} = \left(r_1^{(p-1)}\right)^{p^\sigma} c_1 + \left(r_2^{(p-1)}\right)^{p^\sigma} c_2 + \cdots + \left(r_h^{(p-1)}\right)^{p^\sigma} c_h,$$

so daß also wegen der linearen Unabhängigkeit der c_i über K^{p^σ} notwendig $r_i^{(p-1)} = 0$ sein muß. Die Differentialgleichungen (15) sind mithin in K lösbar, d. h. die Funktion a kann wirklich gemäß den Bedingungen (14) gewählt werden. Damit ist aber in K ein Integral $y = \eta + a$ der Differentialgleichungen (13) mit $\nu \leqq p^\sigma$ gefunden und die Induktion beendet.

Zum Schluß erwähne ich noch den folgenden Satz, dessen Beweis sich jetzt ohne Mühe ergibt:

Satz 13. *Bedeutet*

$$x_1, x_2, \ldots, x_\sigma, \ldots$$

eine Folge von Funktionen aus K, bei der

x_1 *separierend und* $x_\sigma = x_{\sigma-1} + a_\sigma$ *mit* a_σ *aus* kK^{p^σ}

ist, und wird für jede Funktion y aus K

$$\text{im Falle } p^{\sigma-1} \leqq \nu < p^\sigma \qquad \dot{y}^{(\nu)} = D^\nu_{x_\sigma} y$$

gesetzt, so stellt die Zuordnung $y \to \dot{y}^{(\nu)}$ eine iterative Differentiation von K dar, bei der die Elemente von K absolute Differentiationskonstanten sind.

Umgekehrt kann man jede iterative Differentiation von K, bei der die Elemente von k absolute Differentiationskonstanten sind, bei geeigneter Wahl der Folge x_σ auf die angegebene Weise erzeugen.

Eingegangen 22. Februar 1937.

Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques.

Par Mademoiselle *Elisabeth Lutz* à Strasbourg.

Introduction.

Dans l'étude des points rationnels situés sur une courbe algébrique, à coefficients rationnels c'est plutôt le genre, que le degré de la courbe qui intervient. Poincaré [1]) a montré qu'une courbe de genre 1, qui admet un point rationnel peut être ramenée par une transformation birationnelle à coefficients rationnels à la forme canonique $y^2 = x^3 - Ax - B$. On uniformise habituellement la courbe, au moyen de la fonction de Weierstrass, par les formules $x = \wp u$, $y = \frac{1}{2}\wp' u$. Nous savons d'autre part que les arguments elliptiques u des points à coordonnées rationnelles situés sur la courbe forment un module par rapport à l'anneau des entiers ordinaires, et que celui-ci est de base finie [2]).

Il en résulte, que sur les courbes de genre 1, les points rationnels peuvent se déduire par des opérations rationnelles d'un nombre fini d'entre eux.

Mais si l'on considère les solutions (x, y), dans un corps k quelconque, de l'équation $y^2 = x^3 - Ax - B$ d'une cubique de genre 1 (A et B appartenant au corps k), tout ce qu'on sait en général, c'est que ces solutions forment un groupe abélien G [3]). Nous donnerons dans ce travail quelques résultats relatifs au cas où le corps k est un corps $\mathfrak{p}$-adique $k_\mathfrak{p}$. Suivant l'usage [4]), on désignera par $\mathfrak{p} = (\pi)$ l'idéal premier du corps $k_\mathfrak{p}$, par p le nombre premier rationnel qui est multiple de $\mathfrak{p}$; on aura $(p) = \mathfrak{p}^e$, e étant l'ordre de ramification de p dans $k_\mathfrak{p}$; si de plus $N(\mathfrak{p}) = p^f$, le degré de $k_\mathfrak{p}$ par rapport à k_p sera $d = ef$. Soit φ la valuation $\mathfrak{p}$-adique dans $k_\mathfrak{p}$, déterminée par exemple par la condition $\varphi(\pi) = w$ et on sait que l'on a $w < 1$. Alors, A et B étant des entiers de $k_\mathfrak{p}$ tels que $x^3 - Ax - B$ ait son discriminant $\neq 0$, nous étudions la courbe $y^2 = x^3 - Ax - B$, qui est de genre 1. Nous appellerons *point rationnel* sur la courbe tout point (x, y) de la courbe dont les coordonnées sont dans $k_\mathfrak{p}$, ou bien le point à l'infini de la courbe; ces points forment un groupe qui sera appelé G.

A tout point rationnel P de coordonnées (x, y), on fera correspondre le plus petit entier naturel $n = n(P)$ tel que $x\pi^{2n}$ et $y\pi^{3n}$ soient entiers; si P est le point à l'infini on pose $n(P) = +\infty$. Nous démontrerons d'abord que les points P pour lesquels $n(P) \geqq m$ forment un sous-groupe G_m de G, et que ce sous-groupe est d'indice fini. En introduisant, pour les points de G_1, une représentation paramétrique convenable, nous ferons voir en-

[1]) H. Poincaré, Sur les propriétés des courbes algébriques planes, Journal de Liouville (V) **7** (1901), p. 161.

[2]) L. J. Mordell, On the rational solutions of the indeterminate équations of the third and fourth degrees, Proc. of the Cambridge Philos. Soc. **21** (1922), p. 179. Cf. aussi A. Weil, Sur un théorème de Mordell, Bull. Sc. Math. (II) **54** (1930), p. 182.

[3]) Cf. H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Hamb. Abhandl. **10** (1934), p. 325.

[4]) Cf. par exemple C. Chevalley, Sur la théorie des corps de classes, Journal of the Faculty of Science Tokyo **2** (1933).

suite que, dès que m est assez grand (et plus précisément, dès que $4m > e$), G_m est isomorphe au groupe additif des entiers de $k_\mathfrak{p}$; en même temps, nous démontrons que $n(P)$ satisfait aux relations:

$$n(p^r P) = n(P) + ve \qquad n(lP) = n(P) \text{ pour } l \text{ premier à } p$$

valables dès que $4n(P) > e$.

De ce qui précède résulte en particulier, que le point P ne peut être d'ordre fini (dans le groupe G) que si $4n(P) > e$. *Si en particulier $k_\mathfrak{p}$ se réduit au corps p-adique k_p* (d'où $d = e = 1$), *tout point d'ordre fini est à coordonnées entières.* Il est intéressant d'observer qu'on déduit immédiatement de là le même resultat pour le corps des nombres rationnels, si A et B sont des entiers rationnels, tout point rationnel P d'ordre fini sur la cubique $y^2 = x^3 - Ax - B$ de genre 1 est à coordonnées entières.

Dans la deuxième partie nous retrouvons une partie des résultats précédent en définissant d'après A. Weil dans le corps $\mathfrak{p}$-adique, des fonctions analogues aux fonctions elliptiques de l'analyse ordinaire [5]).

Après avoir généralisé aux corps $\mathfrak{p}$-adiques le théorème de Cauchy sur l'existence des solutions d'un système d'équations différentielles, nous définissons au moyen d'un tel système les fonctions dont il s'agit. Elles permettent de démontrer à nouveau l'isomorphie du groupe G_m avec le groupe additif des entiers $\mathfrak{p}$-adiques dès que m est assez grand; et même la limite qu'on obtient pour m par cette méthode, est plus précise que celle que fournit le raisonnement direct, dans le cas où $p \geqq 7$.

Qu'il me soit permis d'exprimer ici ma sincère reconnaissance à M. A. Weil, pour l'aide qu'il m'a apportée au cours de ce travail.

§ 1. Etude algébrique du groupe G.

Le groupe abélien G formé par les points rationnels peut être défini de la manière suivante: à deux points rationnels $P_0(x_0, y_0)$, $P_1(x_1, y_1)$ nous ferons correspondre le point $P_2(x_2, y_2)$ symétrique par rapport à Ox du troisième point d'intersection de la droite P_0P_1 avec la cubique et nous écrirons $P_2 = P_0 + P_1$. On trouve facilement les coordonnées du point P_2 en fonction de celles des points P_0 et P_1; on a en particulier:

$$x_2 = \left(\frac{y_1 - y_0}{x_1 - x_0}\right)^2 - (x_1 + x_0)\,.$$

Si P_1 se confond avec P_0 on prendra au lieu de la droite P_0P_1 la tangente en P_0 à la cubique et l'on écrira $2P_0 = P_2$, avec

$$x_2 = \left(\frac{3x_0^2 - A}{2y_0}\right)^2 - 2x_0\,.$$

Le point $-P_0$ sera le point de coordonneés $(x_0, -y_0)$ et le point à l'infini de la courbe étant considéré comme point rationnel, sera l'unité de notre groupe G.

Tout point rationnel P sur la courbe a des coordonnées de la forme $(\xi\pi^{-2n}, \eta\pi^{-3n})$ n étant un entier rationnel $\geqq 0$, ξ, η étant des entiers de $k_\mathfrak{p}$, *premiers à $\mathfrak{p}$ si $n > 0$*. En effet soit (x, y) un point rationnel: si x est entier $\mathfrak{p}$-adique, y l'est aussi. Si d'autre part $\varphi(x) > 1$, on aura

$\varphi(x^3) = [\varphi(x)]^3 > \varphi(Ax)$ et $\varphi(x^3) > \varphi(B)$ donc $\varphi(y^2) = \varphi(x^3 - Ax - B) = \varphi(x^3)$,

en ce point nous avons donc:

$$\varphi(x) = w^{-2n} \qquad \varphi(y) = w^{-3n}, \qquad n > 0$$

de sorte que les coordonnées x, y sont bien de la forme

$$x = \xi\pi^{-2n} \qquad y = \eta\pi^{-3n}$$

---

[4]) A. Weil, Sur les fonctions elliptiques $\mathfrak{p}$-adiques, Comptes rendus Ac. des Sciences Paris **203** (1936).

avec ξ, η entiers premiers à $\mathfrak{p}$; et ξ, η satisfont à l'équation:

$$\eta^2 = \xi^3 - A\xi\pi^{4n} - B\pi^{6n}.$$

A tout point P correspond ainsi un entier $n \geqq 0$ bien déterminé qu'on désignera par $n(P)$; si P est le point à l'infini on posera $n(P) = \infty$.

Théorème I. *Les points P pour lesquels $n(P) \geqq m$ forment un sous-groupe G_m de G, d'indice fini dans G, quel que soit l'entier $m > 0$.*

Soient en effet deux points rationnels P_0 et P_1, et $P_2 = P_0 + P_1$; et supposons d'abord que $n(P_1) > n(P_0)$ donc $n(P_1) > 0$. Nous pouvons écrire la formule d'addition sous la forme:

$$x_2 = \frac{A(x_0 - x_1) + x_1^2 x_0 - x_0^2 x_1 - 2y_1 y_0}{(x_0 - x_1)^2}$$

d'où

$$\varphi(x_2) = \frac{\varphi(x_1^2 x_0)}{\varphi(x_1^2)} = \varphi(x_0)$$

et par suite:

$$n(P_0 + P_1) = \min[n(P_0), n(P_1)] \quad \text{si} \quad n(P_0) \neq n(P_1).$$

Nous aurions de même

$$n(P_0 - P_1) = \min[n(P_0), n(P_1)] \quad \text{si} \quad n(P_0) \neq n(P_1).$$

Supposons maintenant $n(P_0) = n(P_1)$; nous pouvons écrire $P_0 = P_2 - P_1$; si $n(P_2) \neq n(P_1)$ on aura

$$n(P_0) = \min[n(P_2), n(P_1)]$$

donc $n(P_2) \geqq n(P_0)$. *On a donc en tout cas*:

$$n(P_2) \geqq \min[n(P_0), n(P_1)]$$

ce qui montre bien que G_m est un sous-groupe de G.

Pour démontrer la seconde partie du théorème, nous devons examiner à quelles conditions deux points P_1, P_0 de G doivent satisfaire pour que $P_1 - P_0$ soit dans G_m, c'est-à-dire pour que $n(P_1 - P_0) \geqq m$; nous pouvons supposer que ni P_0 ni P_1 ne soient dans G_m; alors, on devra avoir, tout d'abord, $n(P_0) = n(P_1) = n < m$. Soient $(\xi_0\pi^{-2n}, \eta_0\pi^{-3n})$ et $(\xi_1\pi^{-2n}, \eta_1\pi^{-3n})$ les coordonnées de P_0 et P_1, avec:

$$\eta_0^2 = \xi_0^3 - A\xi_0\pi^{4n} - B\pi^{6n}, \qquad \eta_1^2 = \xi_1^3 - A\xi_1\pi^{4n} - B\pi^{6n}.$$

Il est clair, d'après la formule d'addition, que la condition nécessaire et suffisante pour que $n(P_1 - P_0) \geqq m$, si $n(P_0) = n(P_1) < m$, est que l'on ait:

$$\frac{x_1 - x_0}{y_1 + y_0} (\equiv 0 \bmod \mathfrak{p}^m);$$

c'est-à-dire:

$$\frac{\xi_1 - \xi_0}{\eta_1 + \eta_0} \equiv 0 \pmod{\mathfrak{p}^{m-n}}.$$

Or on a:

$$\frac{\xi_1 - \xi_0}{\eta_1 + \eta_0} = \frac{\eta_1 - \eta_0}{\xi_0^2 + \xi_1\xi_0 + \xi_1^2 - A\pi^{4n}}.$$

Une condition nécessaire, pour que $n(P_1 - P_0) \geqq m$, est donc que

$$\xi_1 \equiv \xi_0, \qquad \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{m-n}}$$

et même cela est suffisant si $n > 0$, car alors, si $p \neq 2$,

$$\eta_1 + \eta_0 \equiv 2\eta_0 \not\equiv 0 \pmod{\mathfrak{p}}$$

et si $p \neq 3$,

$$\xi_0^2 + \xi_0\xi_1 + \xi_1^2 - A\pi^{4n} \equiv 3\xi_0^2 \not\equiv 0 \pmod{\mathfrak{p}}.$$

Il s'ensuit en particulier que G_{m-1}/G_m est un groupe fini, si $m > 1$, donc déjà que G_m est d'indice fini dans G_1. Reste à examiner G/G_1. Pour cela, nous allons faire voir que si $n(P_0) = n(P_1) = 0$, on peut trouver r assez grand pour que $n(P_1 - P_0) \geqq m$ dès que les congruences

$$\xi_1 \equiv \xi_0, \quad \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{r+m}}$$

seront satisfaites.

En effet, si elles le sont et que $n(P_1 - P_0) < m$, on devra avoir, d'après ce qui précède:

$$\eta_1 + \eta_0 \equiv 0, \quad \xi_0^2 + \xi_0\xi_1 + \xi_1^2 - A \equiv 0 \pmod{\mathfrak{p}^r}.$$

On en déduit:

$$2\eta_0 \equiv 0, \quad 3\xi_0^2 - A \equiv 0 \pmod{\mathfrak{p}^r}.$$

Mais on a l'identité:

$$4A^3 - 27B^2 = (x^3 - Ax - B)\,P(x) + (3x^2 - A)\,Q(x)$$

où: $P(x) = -18Ax + 27B$ et $Q(x) = 6Ax^2 - 9Bx - 4A^2$ sont des polynômes à coefficients entiers; en y faisant $x = \xi_0$, on voit donc que

$$2(4A^3 - 27B^2) \equiv 0 \pmod{\mathfrak{p}^r}.$$

Si donc on désigne par $\mathfrak{p}^R$ la plus haute puissance de $\mathfrak{p}$ qui divise $2(4A^3 - 27B^2)$, on voit que les congruences

$$\xi_1 \equiv \xi_0, \quad \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{r+m}}$$

entraînent bien que $n(P_1 - P_0) \geqq m$, pourvu qu'on ait pris $r > R$. Le théorème est ainsi complètement démontré.

Pour aller plus loin, il est utile de se servir d'une représentation paramétrique de la courbe; nous considérons la suivante:

$$x = \frac{1}{t^2}, \quad y = \frac{\varepsilon(t)}{t^3},$$

où $\varepsilon(t)$ est défini par

$$\varepsilon(t) = (1 - At^4 - Bt^6)^{\frac{1}{2}} = 1 + \sum_{\nu=2}^{\infty} \gamma_\nu t^{2\nu}$$

avec $\gamma_2 = -A/2$, $\gamma_3 = -B/2$, etc. Il est clair que si $t \equiv 0 \pmod{\mathfrak{p}^m}$ et si la série $\varepsilon(t)$ est convergente, les formules ci-dessus définissent un point P de la courbe, et que ce point appartient à G_m.

Or on sait que dans la série

$$(1 + u)^{\frac{1}{2}} = 1 + \tfrac{1}{2}u - \tfrac{1}{8}u^2 + \tfrac{1}{16}u^3 - \cdots$$

les dénominateurs des coefficients ne contiennent pas d'autre facteur premier que 2, et que le dénominateur du coefficient de u^ν divise $2^{2\nu}$. Il en résulte que la série $\varepsilon(t)$ converge, si $p \neq 2$, dès que $t \equiv 0 \pmod{\mathfrak{p}}$, et, si $p = 2$, dès que $t \equiv 0 \pmod{\mathfrak{p}^\mu}$, μ étant le plus petit entier plus grand que $\frac{e}{2}$; si $p \neq 2$ nous poserons $\mu = 1$, de sorte qu'en tout cas les formules ci-dessus définissent, pour $t \equiv 0 \pmod{\mathfrak{p}^\mu}$, un point de G_μ. Mais réciproquement, tout point P de G_μ correspond ainsi à une valeur de t, définie par les formules

$$t = \frac{x}{y}\,\varepsilon,$$

$$\varepsilon = \left(1 - \frac{A}{x^2} - \frac{B}{x^3}\right)^{\frac{1}{2}} = 1 + \sum_{2}^{\infty} \gamma_\nu x^{-\nu}$$

la série étant convergente pourvu que P appartienne à G_μ.

Soient maintenant P_0, P_1 deux points de G_μ, correspondant aux valeurs t_0, t_1, du paramètre t; posons $\varepsilon_0 = \varepsilon(t_0)$, $\varepsilon_1 = \varepsilon(t_1)$. Désignons encore par t_2 le paramètre du point $P_2 = P_0 + P_1$; nous allons calculer t_2 en fonction de t_0, t_1. On a d'abord:

$$\frac{y_1 - y_0}{x_1 - x_0} = \frac{\varepsilon_1 t_0^3 - \varepsilon_0 t_1^3}{t_0 t_1 (t_0^2 - t_1^2)} = \frac{t_0^3 - t_1^3 + t_0^3 t_1^3 \sum_{\nu=2}^{\infty} \gamma_\nu (t_1^{2\nu-3} - t_0^{2\nu-3})}{t_0 t_1 (t_0^2 - t_1^2)} = \frac{t_0^2 + t_0 t_1 + t_1^2 - t_0^3 t_1^3 \theta}{t_0 t_1 (t_0 + t_1)}$$

en posant:

$$\theta = \sum_{\nu=2}^{\infty} \gamma_\nu \frac{t_1^{2\nu-3} - t_0^{2\nu-3}}{t_1 - t_0}.$$

Alors la formule d'addition pour x s'écrit:

$$x_2 = \frac{1}{t_2^2} = \frac{1}{(t_0 + t_1)^2} [1 - 2 t_0 t_1 (t_0^2 + t_0 t_1 + t_1^2)\, \theta + t_0^4 t_1^4 \theta^2].$$

L'ambiguité de signe pour t_2 se lève aisèment en considérant aussi y_2; et l'on obtient:

$$\frac{t_2}{t_0 + t_1} = [1 - 2 t_0 t_1 (t_0^2 + t_0 t_1 + t_1^2)\, \theta + t_0^4 t_1^4 \theta^2]^{-\frac{1}{2}}$$

le second membre réprésentant le développement en série qui lui correspond au moyen de la formule du binôme, pourvu que ce développement soit convergent: il en est évidemment ainsi pour $p \neq 2$, car alors θ est entier, et l'on obtient, dans ce cas:

$$\frac{t_2}{t_0 + t_1} \equiv 1 \pmod{\mathfrak{p}^{3n(P_0) + n(P_1)}}$$

en supposant par exemple $n(P_0) \leqq n(P_1)$. On a donc à fortiori, pour $p \neq 2$, chaque fois que P_0, P_1 appartiennent tous deux à G_m:

$$t_2 \equiv t_0 + t_1 \pmod{\mathfrak{p}^{5m}}$$

et en particulier, par récurrence sur l:

$$t(lP_0) = l \cdot t(P_0) \pmod{\mathfrak{p}^{5m}}$$

d'où, pour $l = p$, et si $n(P_0) = n$:

$$\frac{t(pP_0)}{p t(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n-e}}$$

et par récurrence sur ν:

$$\frac{t(p^\nu P_0)}{p^\nu t(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n-e}}$$

donc enfin, en combinant les résultats ci-dessus:

$$\frac{t(lP_0)}{l t(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n-e}}$$

quel que soit l. Il en résulte en particulier que, si $4n(P_0) > e$, l'on aura, si p^ν est la plus haute puissance de p contenue dans l:

$$n(lP_0) = n(P_0) + \nu e.$$

Soit donc, pour $p \neq 2$, α le plus petit entier plus grand que $\frac{e}{4}$; de ce qui précède rés ulte évidemment que, si P_0 appartient à G_α, et si la suite d'entiers ordinaires l_i converge p-adiquement vers un entier p-adique L, les nombres $t(l_i P_0)$ convergeront p-adiquement vers une certaine valeur de t: le point de la courbe qui correspond à celle-ci sera désigné par $L \cdot P$; et l'on voit ainsi que G_α peut être considéré comme un module par rapport à l'anneau des entiers p-adiques.

Pour $p = 2$, on a des résultats semblables, mais un peu moins précis. Une évaluation facile montre que l'on a, si P_0 et P_1 appartiennent à G_m, et pourvu que $m \geqq e$:

$$t_2 \equiv t_0 + t_1 \pmod{\mathfrak{p}^{5m-2e}}$$

résultat qu'on pourrait d'ailleurs encore améliorer quelque peu. On en déduit, comme plus haut:

$$t(lP_0) \equiv lt(P_0) \pmod{\mathfrak{p}^{5m-2e}}$$

$$\frac{t(2P_0)}{2t(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n(P_0)-3e}}$$

$$\frac{t(lP_0)}{lt(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n(P_0)-3e}}$$

et si 2^ν est la plus haute puissance de 2 qui divise l:

$$n(lP_0) = n(P_0) + \nu e$$

pourvu que $n(P_0) \geqq e$. En posant $\alpha = e$ pour $p = 2$, il en résulte, comme plus haut, que G_α peut être considéré comme module par rapport à l'anneau des entiers p-adiques. De là on déduit aussitôt la structure de G_α; plus généralement, on a le théorème suivant.

Théorème II. *Soit β un entier $> \frac{e}{4}$, si $p \neq 2$, et $\geqq e$ si $p = 2$. Alors G_β est isomorphe au groupe additif des entiers $\mathfrak{p}$-adiques.*

Il suffit de faire voir que G_β possède une base de $d = ef$ éléments indépendants par rapport à l'anneau des entiers p-adiques. Pour cela, choisissons, parmi les valeurs de t qui sont $\equiv 0 \pmod{\mathfrak{p}^\beta}$, f valeurs $t_1^{(0)}, t_2^{(0)}, \ldots, t_f^{(0)}$ formant une base minima de $\mathfrak{p}^\beta/\mathfrak{p}^{\beta+1}$; et de même choisissons pour $\varrho = 1, 2, \ldots, e-1$, des valeurs $t_1^{(\varrho)}, t_2^{(\varrho)}, \ldots, t_f^{(\varrho)}$ qui soient $\equiv 0 \pmod{\mathfrak{p}^{\beta+\varrho}}$ et formant une base minima de $\mathfrak{p}^{\beta+\varrho}/\mathfrak{p}^{\beta+\varrho+1}$. Soient $P_i^{(\varrho)}$ les points correspondant à ces ef valeurs de t; et soit $t_i^{(\varrho+\nu e)}$ la valeur t du paramètre, qui correspond au point $P_i^{(\varrho+\nu e)} = p^\nu P_i^{(\varrho)}$. Soient P_0 un point quelconque de G_β, et t_0 son paramétre; il y aura des entiers $n_i^{(0)}$, bien déterminés mod p, tels que

$$t_0 \equiv \sum_i n_i^{(0)} t_i^{(0)} \pmod{\mathfrak{p}^{\beta+1}};$$

alors le point $P_1 = P_0 - \Sigma n_i^{(0)} P_i^{(0)}$ appartiendra à $G_{\beta+1}$, et, s'il correspond à la valeur t_1 du paramètre, il y aura des entiers $n_i^{(1)}$, bien déterminés mod p, tels que

$$t_1 \equiv \sum_i n_i^{(1)} t_i^{(1)} \pmod{\mathfrak{p}^{\beta+2}};$$

en continuant ainsi, on voit que le point

$$P_n = P_0 - \sum_{\nu=0}^{n-1} \sum_i n_i^{(\nu)} P_i^{(\nu)}$$

appartient à $G_{\beta+1}$; et l'on a donc:

$$P_0 = \sum_{\varrho=0}^{e-1} \sum_{i=1}^{f} P_i^{(\varrho)} \left[\sum_{\nu=0}^{\infty} n_i^{(\varrho+\nu e)} p^\nu \right],$$

on voit en même temps que cette expression de P_0 est unique, de sorte que le théorème est démontré.

Une conséquence intéressante des résultats ci-dessus, c'est qu'un point P de G ne peut être d'ordre fini dans G s'il appartient à G_β; en particulier, *si $e = 1$, un point P d'ordre fini dans G est à coordonnées entières.*

Si maintenant nous considérons les solutions, *dans le corps des nombres rationnels ordinaires*, d'une équation $y^2 = x^3 - Ax - B$ à coefficients entiers rationnels, elles

forment un groupe qui est contenu dans le groupe des solutions p-adiques de la même équation, et cela quel que soit p. Une solution en nombres rationnels ne peut donc être d'ordre fini que si x et y sont entiers dans tout corps p-adique, c'est-à-dire s'ils sont entiers rationnels. Cela étant, la détermination effective de ces solutions est fournie par le théorème suivant:

Théorème III. *Soit $y^2 = x^3 - Ax - B$ une cubique de genre 1 à coefficients entiers rationnels. Tout point $P(x, y)$ à coordonnées rationnelles, et d'ordre fini dans le groupe des points rationnels sur la cubique, est à coordonnées entières, et tel que y^2 soit égal à 0 ou à un diviseur de $4A^3 - 27B^2$.*

La première partie étant déjà démontrée, considérons le second point. Si P est d'ordre fini, il en est de même de $2P$, qui doit donc être aussi à coordonnées entières s'il n'est à l'infini; ce dernier cas se présente si $y = 0$; s'il n'en est pas ainsi il faut et il suffit, pour qu'il soit à coordonnées entières, que l'on ait:

$$3x^2 - A \equiv 0 \pmod{2y}.$$

Mais on a l'identité:

$$(3x^2 - A)^2 (3x^2 - 4A) \equiv -4A^3 + 27B^2 \pmod{x^3 - Ax - B}$$

et par conséquent, dans le cas présent:

$$-4A^3 + 27B^2 \equiv 0 \pmod{y^2}$$

ce qu'il fallait démontrer.

§ 2. Les fonctions elliptiques $\mathfrak{p}$-adiques.

On peut obtenir une partie des résultats précédents par une autre méthode en utilisant les fonctions elliptiques $\mathfrak{p}$-adiques définies par A. Weil [5]). Nous allons reprendre cette définition, en l'étendant au cas $p = 2$.

Nous définirons d'une façon formelle la dérivée d'une fonction développée en série entière: par le développement dérivé, ceci est possible puisque ce développement est convergent dans le corps $\mathfrak{p}$-adique dès que le premier l'est. Dans ces conditions les propriétés habituelles de la dérivation sont encore valables.

Nous commencerons par donner une démonstration générale du théorème d'existence des solutions d'un système d'équations différentielles dans le corps $\mathfrak{p}$-adique, théorème que l'on peut énoncer de la manière suivante.

Théorème IV. *Soit un système d'équations différentielles*

$$\frac{dy_i}{dx} = F_i(x, y_1, y_2, \ldots, y_n) \qquad (i = 1, 2, \ldots, n) \tag{1}$$

les F_i étant des séries de puissances en $x, y_1, \ldots, y_n$ à coefficients dans $k_\mathfrak{p}$ convergentes dans un certain voisinage $\mathfrak{p}$-adique de $x = y_i = 0$. Ce système admet une solution et une seule de la forme $y_i = f_i(x)$ telle que $f_i(0) = 0$, les f_i étant des séries de puissances de x convergentes dans un certain voisinage de $x = 0$.

Posons en effet:

$$F_i(x, y_1, \ldots, y_n) = \sum a^{(i)}_{\mu\nu_1\ldots\nu_n} x^\mu y_1^{\nu_1} \cdots y_n^{\nu_n}$$

les coefficients a étant des nombres de $k_\mathfrak{p}$.

Le deuxième membre, série entière par rapport aux puissances positives croissantes de x et des y_i, est supposé convergent dans le corps $\mathfrak{p}$-adique dès que:

$$x \equiv 0 \pmod{\mathfrak{p}^\alpha}, \qquad y_i \equiv 0 \pmod{\mathfrak{p}^{\beta_i}}. \tag{2}$$

Dans chacune des séries F_i, tous les termes, sauf un nombre fini d'entre eux, sont des entiers $\mathfrak{p}$-adiques dès que x et y satisfont à (2), ou en d'autres termes les nombres

$$a^{(i)}_{\mu\nu_1\cdots\nu_n}\,\pi^{\mu\alpha+\nu_1\beta_1+\cdots+\nu_n\beta_n}$$

sont entiers à l'exception au plus d'un nombre fini d'entre eux; et par suite on peut trouver ϱ_i tels que ces nombres deviennent entiers si on les multiplie par π^{ϱ_i}.

Faisons alors dans les équations proposées la transformation:

$$x = \pi^{\gamma} x', \qquad y_i = \pi^{\beta_i} y'.$$

Les coefficients des nouvelles équations seront

$$a^{(i)}_{\mu\nu_1\nu_2\cdots\nu_n}\,\pi^{\gamma-\beta_i+\mu\gamma+\nu_1\beta_1+\cdots+\nu_n\beta_n}$$

et ils seront tous entiers si l'on prend pour γ le plus grand des nombres α, $\beta_i + \varrho_i$.

Nous sommes donc ramenés au cas où tous les coefficients des séries F_i sont entiers.

Or les équations (1) nous permettent par différentiations successives de calculer formellement les dérivées d'un ordre quelconque de y_i par rapport à x pour $x = 0$, qui seront des polynômes à coefficients numériques entiers par rapport aux coefficients $a^{(i)}_{\mu\nu_1\cdots\nu_n}$ des séries F_i; les séries

$$(3) \qquad y_i = \left(\frac{dy_i}{dx}\right)_0 x + \left(\frac{d^2y_i}{dx^2}\right)_0 \frac{x_2}{2!} + \cdots + \left(\frac{d^ny_i}{dx^n}\right)_0 \frac{x^n}{n!} + \cdots$$

satisfont formellement aux équations (1). Mais elles convergent en même temps que la série exponentielle c'est-à-dire pour $x \equiv 0 \pmod{\mathfrak{p}^{\varrho}}$ si $\varrho > \dfrac{e}{p-1}$. Le théorème est donc démontré.

Ce résultat va nous permettre de définir dans le corps $\mathfrak{p}$-adique $k_{\mathfrak{p}}$ des fonctions analogues aux fonctions elliptiques de l'analyse ordinaire. Habituellement on exprime les coordonnées x, y d'un point de la courbe $y^2 = x^3 - Ax - B$ par les formules $x = \wp u$, $y = \frac{1}{2}\wp' u$; pour obtenir une représentation semblable dans $k_{\mathfrak{p}}$ le plus commode sera de se servir de la fonction auxiliaire $t(u) = (\wp u)^{-\frac{1}{2}}$ qui n'est pas autre chose que le paramètre t dont nous nous sommes servis au § 1; en analyse ordinaire cette fonction satisfait à l'équation différentielle

$$\frac{dt}{du} = (1 - At^4 - Bt^6)^{\frac{1}{2}}.$$

Plaçons-nous maintenant dans le corps $\mathfrak{p}$-adique, et considérons l'équation différentielle

$$\frac{dt}{du} = (1 - At^4 - Bt^6)^{\frac{1}{2}} = 1 + \sum_{\nu=2}^{\infty} \gamma_\nu t^{2\nu}.$$

D'après le théorème IV, cette équation définit une fonction $t(u)$ telle que $t(0) = 0$, développable suivant les puissances entières de u:

$$t(u) = \sum_1^{\infty} \frac{1}{\nu!}\left(\frac{d^\nu t}{du^\nu}\right)_0 u^\nu = u - \frac{A}{10}u^5 - \frac{B}{14}u^7 + \cdots$$

le développement étant convergent dans un voisinage de $u = 0$ qu'il est facile de déterminer. En effet, soit ϱ, comme plus haut, le plus petit entier $> \dfrac{e}{p-1}$; si $p \neq 2$ l'équation différentielle est à coefficients entiers, et la série $t(u)$ converge pour $u \equiv 0 \pmod{\mathfrak{p}^{\varrho}}$; si $p \neq 2$ on transformera l'équation différentielle en une équation à coefficients entiers

par le changement de variables $t = \pi^\lambda t'$, $u = \pi^\lambda u'$ si λ est le plus petit entier $\geqq \frac{e}{2}$, donc la série $t'(u')$ converge pour $u' \equiv 0 \pmod{\mathfrak{p}^\varrho}$, et $t(u)$ converge pour $u \equiv 0 \pmod{\mathfrak{p}^{\varrho+\lambda}}$.

De plus, considérons, pour $p \neq 2$, la série

$$\frac{t(u)}{u} - 1 = \sum_5^\infty \frac{1}{\nu!}\left(\frac{d^\nu t}{du^\nu}\right)_0 u^{\nu-1}$$

on vérifie facilement que tous ses termes sont $\equiv 0 \pmod{\mathfrak{p}}$ pourvu que $u \equiv 0 \pmod{\mathfrak{p}^{\varrho'}}$, ϱ' désignant le plus petit entier tel que

$$\varrho' > \frac{p^2 e}{(p^2-1)(p-1)}$$

et de même, pour $p = 2$, la série $\frac{t'(u')}{u'} - 1$ a tous ses termes $\equiv 0 \pmod{\mathfrak{p}}$ si $u' \equiv 0 \pmod{\mathfrak{p}^{\varrho'}}$, ϱ' étant le plus petit entier $> \frac{9e}{8}$. Désignons donc par σ l'entier ϱ' si $p \neq 2$ et l'entier $\varrho' + \lambda$ si $p = 2$; on voit qu'en tout cas, si

$$u \equiv 0 \pmod{\mathfrak{p}^\sigma}$$

la fonction $t(u)$ est définie et telle que

$$\frac{t(u)}{u} \equiv 1 \pmod{\mathfrak{p}}.$$

A partir de cette fonction $t(u)$, nous pouvons maintenant, pour $u \equiv 0 \pmod{\mathfrak{p}^\sigma}$, définir les fonctions

$$\wp u = \frac{1}{t^2(u)}, \qquad \wp' u = \frac{-2}{t^3(u)}\frac{dt}{du}$$

qui satisfont évidemment à l'équation

$$\frac{1}{4}\wp'^2 u = \wp^3 u - A\wp u - B$$

de sorte que le point

$$x = \wp u, \qquad y = \frac{1}{2}\wp' u$$

est un point de la courbe $y^2 = x^3 - Ax - B$, et plus précisément un point du groupe G_m si $u \equiv 0 \pmod{\mathfrak{p}^m}$ et $m \geqq \sigma$. Et réciproquement, tout point de G_m correspond ainsi à une valeur de u et une seule; car on a vu dans le § 1 qu'à tout point P de G_m correspond, si $m \geqq \mu$ (avec $\mu = 1$ pour $p \neq 2$ et μ étant le plus petit entier $> \frac{e}{2}$ si $p = 2$) une valeur de t bien déterminée, $\equiv 0 \pmod{\mathfrak{p}^m}$; alors u est déterminé au moyen de t par l'équation

$$\frac{du}{dt} = (1 - At^4 - Bt^6)^{-\frac{1}{2}}$$

d'où

$$u(t) = \int_0^t (1 - At^4 - Bt^6)^{-\frac{1}{2}}\, dt = t + \frac{A}{10}t^5 + \frac{B}{14}t^7 + \cdots$$

et l'on vérifie immédiatement que la série $u(t)$ est convergente, et a tous ses termes, à partir du second, $\equiv 0 \pmod{\mathfrak{p}^\sigma}$, pour $t \equiv 0 \pmod{\mathfrak{p}^\sigma}$.

Enfin, considérons le théorème d'addition auxquelles satisfont, en analyse ordinaire, $\wp u$ et $\wp' u$: ce théorème s'exprime par des identités algébriques auxquelles satisfont les coefficients du développement en série de $t(u)$, coefficients qui sont des polynômes en A, B à coefficients numériques rationnels; il reste donc valable en analyse $\mathfrak{p}$-adique. On en déduit que si les points P_0, P_1 de G correspondent aux valeurs u_0, u_1 du paramètre u, le point $P_2 = P_0 + P_1$ correspond à $u_2 = u_0 + u_1$. *Il y a donc isomorphie entre* G_σ *et le groupe additif des nombres* $u \equiv 0 \pmod{\mathfrak{p}^\sigma}$: c'est là un résultat moins précis que celui du théorème II pour $p = 2, 3, 5$, mais plus précis dès que $p \geqq 7$.

Eingegangen 28. Dezember 1936.

Alfred Ackermann-Teubner-Gedächtnispreis 1937.

Der von Herrn Domherrn Dr. Dr. Ing. Alfred Ackermann-Teubner in Leipzig im Jahre 1912 der Universität Leipzig gestiftete „Alfred Ackermann-Teubner-Gedächtnispreis zur Förderung der Mathematischen Wissenschaften" in Höhe von RM 500.— ist im Jahre 1937 durch das Preisgericht dem Professor für theoretische Physik in Rostock Dr. Pascual Jordan für seine hervorragenden Arbeiten auf dem Gebiete der modernen Atomphysik zuerkannt worden.

Über die Galoissche Gruppe der Hermiteschen Polynome.

Von *Werner Schulz* in Berlin.

In der vorliegenden Arbeit soll gezeigt werden, daß folgende von Herrn I. Schur ausgesprochene und für $n > 12$ bewiesene Vermutung [1]) auch für $n \leqq 12$ richtig ist:

Satz. *Bedeutet*

$$H_m(x) = (-1)^m e^{\frac{x^2}{2}} \frac{d^m}{dx^m}\left(e^{-\frac{x^2}{2}}\right) = \sum_{\mu=0}^{\left[\frac{m}{2}\right]} (-1)^\mu \binom{m}{2\mu} 1 \cdot 3 \cdot 5 \cdots (2\mu - 1)\, x^{m-2\mu}$$

das m-te Hermitesche Polynom und setzt man

$$H_{2n}(x) = K_n^{(0)}(x^2), \qquad H_{2n+1}(x) = x\, K_n^{(1)}(x^2),$$

so ist die Galoissche Gruppe der Gleichungen

$$K_n^{(\varepsilon)}(x) = 0 \qquad (\varepsilon = 0, 1)$$

die symmetrische Gruppe $\mathfrak{S}_n$.

§ 1. Hilfsmittel für den Beweis.

Bei den Schurschen Untersuchungen spielt folgendes Kriterium eine wichtige Rolle:

Es liege eine Gleichung n-ten Grades $F(x) = 0$ mit ganzen rationalen Koeffizienten vor, die folgende Bedingungen erfüllt:

a) Die Funktion $F(x)$ ist im Körper der rationalen Zahlen irreduzibel.

b) Die Diskriminante der Gleichung $F(x) = 0$ enthält eine Primzahl p mindestens in der n-ten Potenz.

c) Das konstante Glied von $F(x)$ ist durch p, aber nicht durch p^2 teilbar.

d) Es gilt eine Kongruenz der Form

$$F(x) \equiv x^k f(x) \pmod{p} \qquad (k > 1),$$

wobei die Diskriminante des Polynoms $f(x)$ zu p teilerfremd ist.

Dann besitzt die Galoissche Gruppe der Gleichung eine durch p teilbare Ordnung.

Mit Hilfe dieses Kriteriums gelingt es zu zeigen, daß die Ordnung $g_n^{(\varepsilon)}$ der Galoisschen Gruppe $\mathfrak{G}_n^{(\varepsilon)}$ von $K_n^{(\varepsilon)}(x) = 0$ durch jede Primzahl p des Intervalls

$$\frac{2n + 2\varepsilon}{3} < p < n$$

[1]) I. Schur, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome, dieses Journal **165** (1931), S. 52—58.

teilbar sein muß.

Da nun eine Gruppe des Grades n, in deren Ordnung eine Primzahl p des Intervalls

$$\frac{n}{2} < p < n - 2$$

aufgeht, die alternierende oder symmetrische Gruppe n-ten Grades ist, so umfaßt $\mathfrak{G}_n^{(\varepsilon)}$ die alternierende Gruppe $\mathfrak{A}_n$, sobald eine Primzahl p mit

$$\frac{2n + 2\varepsilon}{3} < p < n - 2$$

existiert. Dies trifft für alle $n > 13$ mit Ausnahme von $n = 19$, $\varepsilon = 1$ zu. So erkennt man für diese Fälle die Affektlosigkeit der Gleichungen $K_n^{(\varepsilon)}(x) = 0$, wenn man noch beachtet, daß die Diskriminante

$$(1) \quad \Delta_n^{(\varepsilon)} = 2^{\frac{n(n-1)}{2}} \cdot 2^2 \cdot 3^3 \cdots n^n (3 + 2\varepsilon)(5 + 2\varepsilon)^2 \cdots (2n - 1 + 2\varepsilon)^{n-1}$$

von $K_n^{(\varepsilon)}(x)$ keine Quadratzahl ist [2]).

Für die kleinen Werte von n lassen sich die beim Beweis benötigten Primzahlbedingungen nicht mehr verwirklichen. Man hat hier die Möglichkeit, Permutationen aus $\mathfrak{G}_n^{(\varepsilon)}$ zu finden, wenn man folgenden Satz von Dedekind heranzieht:

Ist $F(x)$ ein Polynom mit ganzen rationalen Koeffizienten und dem höchsten Koeffizienten 1 und gilt für eine Primzahl p die Zerlegung

$$F(x) \equiv F_1(x) F_2(x) \cdots F_r(x) \pmod{p},$$

wobei die Faktoren $F_\varrho(x) \pmod{p}$ irreduzibel und untereinander inkongruent sind, so enthält die Galoissche Gruppe der Gleichung $F(x) = 0$ eine Permutation, die in r Zyklen zerfällt, deren Ordnungen die Gradzahlen der $F_\varrho(x)$ sind.

Dieser Satz kann zur Bestimmung der Galoisschen Gruppe benutzt werden in Verbindung mit dem folgenden:

Eine primitive Gruppe $\mathfrak{G}$ des Grades n, die einen Zyklus der Primzahlordnung q enthält, ist mindestens $(n - q + 1)$-fach transitiv. Ist $q = 2$, so ist $\mathfrak{G} = \mathfrak{S}_n$; für $q = 3$ muß $\mathfrak{A}_n$ in $\mathfrak{G}$ liegen.

Für die praktische Anwendung des Dedekindschen Satzes im Fall der Gleichungen $K_n^{(\varepsilon)}(x) = 0$ ergeben sich einige Unannehmlichkeiten. Zunächst sind die kleinen Primzahlen für die Benutzung unbrauchbar; denn ein Primzahlmodul, für den der Satz anwendbar sein soll, darf nicht in der Diskriminante der Gleichung aufgehen, muß also im vorliegenden Fall nach (1) größer als $2n - 1 + 2\varepsilon$ sein. Ferner kommt hinzu, daß das Auffinden eines irreduziblen Faktors von $K_n^{(\varepsilon)}(x) \pmod{p}$, der nicht linear oder quadratisch ist, mit einem recht erheblichen Rechenaufwand verbunden sein kann.

Diese Schwierigkeiten für die Bestimmung von $\mathfrak{G}_n^{(\varepsilon)}$ in den bei Herrn Schur nicht erledigten Fällen lassen sich nun beheben, wenn man eine Verschärfung des Schurschen Kriteriums benutzt, die ich in meiner Dissertation aufgestellt habe [3]):

Es liege eine Gleichung n-ten Grades $F(x) = 0$ mit ganzen rationalen Koeffizienten vor, die folgende Bedingungen erfüllt:

a) $F(x)$ ist im Körper der rationalen Zahlen irreduzibel.

b) Das konstante Glied von $F(x)$ enthält eine Primzahl p genau im Quadrat.

---

[2]) Die in dieser Arbeit als bekannt angegebenen Tatsachen über $K_n^{(\varepsilon)}(x)$ sind bei Herrn Schur a. a. O. [1]) bewiesen.

[3]) Werner Schulz, Reduzibilität, Irreduzibilität und Affektfreiheit bei gewissen Klassen von Polynomen, Schriften d. Math. Seminars u. d. Inst. f. angew. Math. d. Universität Berlin **3** (1937), S. 117—154, insbes. S. 138—140.

c) Es gilt

$$F(x) \equiv x^k \psi(x) \pmod{p} \qquad (k > 1),$$

wobei die Diskriminante von $\psi(x)$ zu p teilerfremd ist.

d) Es gilt

$$F(x) \equiv x^l \chi(x) \pmod{p^2} \qquad \left(l < \frac{k}{2}\right),$$

wobei $\chi(x) \not\equiv 0 \pmod{p^2, x}$ ist.

e) Die Diskriminante von $F(x)$ enthält p mindestens in der $(n + 2l)$-ten Potenz.

Dann besitzt die Galoissche Gruppe der Gleichung eine durch p teilbare Ordnung.

Mit diesem Kriterium kann man für einen Teil der bisher offen gelassenen Fälle die Richtigkeit des eingangs genannten Satzes nachweisen, für die restlichen Fälle liefert der Dedekindsche Satz das gesuchte Ergebnis.

§ 2. Ein Hilfssatz über die Primteiler von $g_n^{(\varepsilon)}$.

Hilfssatz. Die Ordnung $g_n^{(\varepsilon)}$ der Galoisschen Gruppe $\mathfrak{G}_n^{(\varepsilon)}$ von $K_n^{(\varepsilon)}(x) = 0$ ist durch jede Primzahl p des Intervalls

$$\frac{n+2}{2} \leqq p \leqq \frac{2n-1+2\varepsilon}{3} \qquad (p > 3) \tag{2}$$

teilbar. (Außerdem ist bekannt (vgl. § 1), daß $g_n^{(\varepsilon)}$ durch jede Primzahl des Intervalls $\frac{2n+2\varepsilon}{3} < p < n$ teilbar ist.)

Beweis. Es soll gezeigt werden, daß für jedes p aus (2) die Voraussetzungen a) bis e) des im vorigen Paragraphen zuletzt genannten Kriteriums zutreffen. Dann ist die Richtigkeit des Hilfssatzes sichergestellt.

$K_n^{(\varepsilon)}(x)$ ist bekanntlich im Körper der rationalen Zahlen irreduzibel; somit gilt a).

Für die übrigen Bedingungen des Kriteriums ist festzustellen, in welcher Potenz p in den Koeffizienten von $K_n^{(\varepsilon)}(x)$ auftritt. Der Koeffizient von $x^{n-\nu}$ in $K_n^{(\varepsilon)}(x)$ ist

$$a_\nu^{(\varepsilon)} = (-1)^\nu \binom{2n+\varepsilon}{2\nu} 1 \cdot 3 \cdot 5 \cdots (2\nu - 1) = \frac{(-1)^\nu}{2^\nu} \frac{(2n+\varepsilon)!}{(2n-2\nu+\varepsilon)!\,\nu!}. \tag{3}$$

Die höchste Potenz von p, die in $a_\nu^{(\varepsilon)}$ aufgeht, sei $t_\nu^{(\varepsilon)}$. Dann wird behauptet:

$$t_\nu^{(\varepsilon)} = 0 \quad \text{für} \quad \nu = n - \frac{3p+1-2\varepsilon}{2}, \tag{4}$$

$$t_\nu^{(\varepsilon)} \geqq 1 \quad \text{für} \quad n - \frac{3p+1-2\varepsilon}{2} < \nu < n - \frac{p+1-2\varepsilon}{2}, \tag{5}$$

$$t_\nu^{(\varepsilon)} = 1 \quad \text{für} \quad \nu = n - \frac{p+1-2\varepsilon}{2}, \tag{6}$$

$$t_\nu^{(\varepsilon)} = 2 \quad \text{für} \quad n - \frac{p+1-2\varepsilon}{2} < \nu \leqq n. \tag{7}$$

Für $\nu = n - \frac{3p+1-2\varepsilon}{2}$ folgt nämlich aus (2)

$$\begin{gathered} 3p \leqq 2n + \varepsilon < 4p, \\ 3p \leqq 2n - 2\nu + \varepsilon = 3p + 1 - \varepsilon < 4p, \\ 0 \leqq \nu = n - \frac{3p+1-2\varepsilon}{2} < p. \end{gathered} \tag{8}$$

Folglich geht p wegen (3) in dem zugehörigen $a_\nu^{(\varepsilon)}$ nicht auf, d. h. es gilt (4).

Ist $v = n - \frac{3p+1-2\varepsilon}{2} + \delta$ $(\delta = 1, 2, \ldots, p)$, so bestehen außer (8) die Ungleichungen

$$p \leqq 2n - 2v + \varepsilon = 3p + 1 - \varepsilon - 2\delta < 3p,$$

$$0 < v = n - \frac{3p+1-2\varepsilon}{2} + \delta < 2p.$$

Man unterscheide nun, was nach (2) möglich ist:

$\alpha)$ $\quad \delta \leqq \frac{p+1-\varepsilon}{2}$. Dann ist $t_v^{(\varepsilon)} = 1$.

$\beta)$ $\quad \frac{p+1-\varepsilon}{2} < \delta < \frac{5p-2n+1-2\varepsilon}{2}$. Dann ist $t_v^{(\varepsilon)} = 2$.

$\gamma)$ $\quad \delta \geqq \frac{5p-2n+1-2\varepsilon}{2}$. Dann ist $t_v^{(\varepsilon)} = 1$.

Das zeigt die Richtigkeit von (5) und (6).

Ist $v = n - \frac{p+1-2\varepsilon}{2} + \delta$ $\left(\delta = 1, 2, \ldots, \frac{p+1-2\varepsilon}{2}\right)$, so gilt außer (8)

$$0 \leqq 2n - 2v + \varepsilon = p + 1 - \varepsilon - 2\delta < p,$$

$$p < v = n - \frac{p+1-2\varepsilon}{2} + \delta < 2p.$$

Hieraus folgt (7), und insbesondere erkennt man die Gültigkeit von b).

Aus (4), (5), (6) und (7) ergibt sich

$$K_n^{(\varepsilon)}(x) \equiv x^{\frac{3p+1-2\varepsilon}{2}} \psi^{(\varepsilon)}(x) \pmod{p}.$$

Eine einfache Rechnung lehrt ferner, daß

$$\psi^{(0)}(x) \equiv K^{(1)}_{n-\frac{3p+1}{2}}(x) \pmod{p},$$

$$\psi^{(1)}(x) \equiv K^{(0)}_{n-\frac{3p-1}{2}}(x) \pmod{p}$$

ist. Nun ist die Diskriminante $\Delta_n^{(\varepsilon)}$ von $K_n^{(\varepsilon)}(x)$ nach (1) nur durch Primzahlen teilbar, die nicht größer als $2n - 1 + 2\varepsilon$ sind. Da wegen (2)

$$p \geqq 2n - 3p + 4$$

ist, so wird die Diskriminante von $\psi^{(\varepsilon)}(x)$ zu p teilerfremd. Also besteht c) mit $k = \frac{3p+1-2\varepsilon}{2} > 1$.

Weiter ist

$$K_n^{(\varepsilon)}(x) \equiv x^{\frac{p+1-2\varepsilon}{2}} \chi^{(\varepsilon)}(x) \pmod{p^2},$$

wo $\chi^{(\varepsilon)}(x) \not\equiv 0 \pmod{p^2, x}$ ist, d. h. es gilt d) mit $l = \frac{p+1-2\varepsilon}{2} < \frac{k}{2}$.

In $\Delta_n^{(\varepsilon)}$ treten wegen (2) die Faktoren p^p, $p^{\frac{p-1-2\varepsilon}{2}}$ und $(3p)^{\frac{3p-1-2\varepsilon}{2}}$ auf. Da

$$p + \frac{p-1-2\varepsilon}{2} + \frac{3p-1-2\varepsilon}{2} = 3p - 1 - 2\varepsilon \geqq n + 2 + p - 1 - 2\varepsilon = n + 2l$$

ist, so ist auch e) erfüllt.

§ 3. Beweis des Satzes für $n \leqq 12$.

Die Gruppe $\mathfrak{G}_n^{(\varepsilon)}$ ist transitiv und kann nicht $\mathfrak{A}_n$ sein, da $\Delta_n^{(\varepsilon)}$ keine Quadratzahl ist. Es ist also zu beweisen, daß $\mathfrak{A}_n$ in $\mathfrak{G}_n^{(\varepsilon)}$ enthalten ist.

$n = 2$ und 3. Hier ist die Richtigkeit der Behauptung trivial.

$n = 4$. Es ist $g_4^{(0)} \equiv 0 \pmod 3$, was auf $\mathfrak{A}_4 < \mathfrak{G}_4^{(0)}$ führt. Für $\varepsilon = 1$ ist man auf den Dedekindschen Satz angewiesen. Da in der Zerlegung

$$K_4^{(1)}(x) \equiv (x-5)\,(x^3+2x^2+3x-2) \pmod{11}$$

die Faktoren mod 11 irreduzibel sind, so muß $\mathfrak{G}_4^{(1)}$ einen Dreierzyklus und somit $\mathfrak{A}_4$ enthalten.

$n = 5$. Auch hier kann noch nicht der Hilfssatz benutzt werden, da in dem Intervall $\frac{5+2}{2} \leqq p < 5$ keine Primzahl vorhanden ist. $\mathfrak{G}_5^{(\varepsilon)}$ ist als Gruppe von Primzahlgrad primitiv und enthält einen Dreierzyklus, da in den Zerlegungen

$$K_5^{(0)}(x) \equiv (x-6)\,(x+7)\,(x^3+5x^2+4x-3) \pmod{17},$$
$$K_5^{(1)}(x) \equiv (x-1)\,(x+6)\,(x^3+5x^2-4x-3) \pmod{13}$$

die Faktoren irreduzibel sind. Also ist $\mathfrak{A}_5 < \mathfrak{G}_5^{(\varepsilon)}$.

$n = 6$. Es ist $g_6^{(\varepsilon)} \equiv 0 \pmod 5$, was die Primitivität von $\mathfrak{G}_6^{(\varepsilon)}$ nach sich zieht. Ferner bestehen folgende Zerlegungen in irreduzible Bestandteile:

$$K_6^{(0)}(x) \equiv (x+13)\,(x^2+8x-7)\,(x^3+6x^2-9x+5) \pmod{31},$$
$$K_6^{(1)}(x) \equiv (x-4)\,(x^2+9x+7)\,(x^3-7x^2+5x-5) \pmod{19}.$$

Da $\mathfrak{G}_6^{(\varepsilon)}$ hiernach eine Permutation der Form $(\alpha_1, \alpha_2)\,(\beta_1, \beta_2, \beta_3)$, also auch eine Transposition enthält, so ist $\mathfrak{G}_6^{(\varepsilon)} = \mathfrak{S}_6$.

$n = 7$ und 8. Auf Grund des Hilfssatzes ist $g_n^{(\varepsilon)} \equiv 0 \pmod 5$, und daher muß $\mathfrak{A}_n < \mathfrak{G}_n^{(\varepsilon)}$ sein.

$n = 9$. Es ist $g_9^{(\varepsilon)} \equiv 0 \pmod 7$, woraus die Primitivität von $\mathfrak{G}_9^{(\varepsilon)}$ folgt. Ferner gilt

$$K_9^{(0)}(x) \equiv (x-3)\,(x+11)\,(x^2+18x+11)\,(x^5+9x^4-12x^3+17x^2-19x-19) \pmod{47},$$
$$K_9^{(1)}(x) \equiv (x-5)\,(x-17)\,(x^2+33x-17)\,(x^5+19x^4+17x^3+2x^2+6x+26) \pmod{67}.$$

In beiden Zerlegungen kommt kein weiterer Linearfaktor vor; dagegen könnten die Faktoren fünften Grades noch in einen quadratischen und kubischen Faktor zerfallen. In jedem Fall enthält $\mathfrak{G}_9^{(\varepsilon)}$ eine Permutation, von der eine geeignete Potenz eine Transposition oder einen Dreierzyklus liefert. Somit ist $\mathfrak{A}_9 < \mathfrak{G}_9^{(\varepsilon)}$.

$n = 10, 11, 12$. Nach dem Hilfssatz ist $g_n^{(\varepsilon)} \equiv 0 \pmod 7$ und folglich $\mathfrak{A}_n < \mathfrak{G}_n^{(\varepsilon)}$.

Auch der bei Herrn Schur nur unter Benutzung genauerer Ergebnisse über die möglichen primitiven Permutationsgruppen des Grades 18 bewiesene Fall $n = 19$, $\varepsilon = 1$ ist nach dem Hilfssatz wegen $g_{19}^{(1)} \equiv 0 \pmod{13}$ sofort zu erledigen.

Eingegangen 10. Februar 1937.

Neue Bände der Sammlung Göschen:

Band 1110:

Formelsammlung zur praktischen Mathematik

Von Dr. habil. Günther Schulz, Assistent am Institut für angewandte Mathematik an der Universität Berlin. Mit 10 Abbildungen. 147 Seiten.

Band 1109:

Elemente der Funktionentheorie

Von Professor Dr. Konrad Knopp, o. ö. Professor der Mathematik an der Universität Tübingen. Mit 23 Figuren. 144 Seiten.

Band 668:

Funktionentheorie

Von Professor Dr. Konrad Knopp, o. ö. Professor der Mathematik an der Universität Tübingen. Erster Teil: Grundlagen der allgemeinen Theorie der analytischen Funktionen. Fünfte, vollständig neu bearbeitete Auflage. Mit 8 Figuren. 136 Seiten.

Band 932:

Höhere Algebra

Von Dr. Helmut Hasse, o. ö. Professor der Mathematik an der Universität Göttingen. II. Gleichungen höheren Grades. 2., verbesserte Auflage. Mit 5 Figuren. 158 Seiten.

Band 768:

Einführung in die konforme Abbildung

Von Dr. Ludwig Bieberbach, Mitglied der Preuß. Akademie der Wissenschaften, o. ö. Professor an der Universität Berlin. Dritte Auflage. Mit 42 Zeichnungen. 137 Seiten.

Band 180:

Versicherungsmathematik

Von Dr. Friedrich Böhm, Professor an der Universität München. I. Elemente der Versicherungsrechnung. Zweite, vermehrte und verbesserte Auflage. 152 Seiten.

Jeder Band in Leinen gebunden RM 1.62

Sammelbezugspreise: 10 Exemplare RM 14.40, 25 Exemplare RM 33.75, 50 Exemplare RM 63.—

Walter de Gruyter & Co., Berlin W 35, Woyrschstr. 13

Handbuch der neuzeitlichen Wehrwissenschaften

Herausgegeben im Auftrage der Deutschen Gesellschaft für Wehrpolitik und Wehrwissenschaften und unter Mitarbeit zahlreicher Sachverständiger von

HERMANN FRANKE
Generalmajor a. D.

4 Bände. Lexikon-Oktav.

Soeben ist erschienen:

2. Band: **Das Heer**

Mit einem Geleitwort von Generaloberst Freiherr von Fritsch, XII, 804 Seiten. 1937.

1936 ist erschienen:

1. Band: **Wehrpolitik und Kriegführung**

Mit einem Geleitwort von Reichskriegsminister Generalfeldmarschall von Blomberg. Mit 81 farbigen und schwarzen Tafeln und 147 Skizzen im Text. XIII, 749 Seiten.

Subskriptionspreis bei Bezug aller vier Bände gebunden je RM 32.—, bei Einzelbezug gebunden RM 36.—.

In Vorbereitung befinden sich:

Band 3: **Kriegsmarine und Luftwaffe.**

Band 4: **Wehrwirtschaft und Wehrtechnik.**

„ . . . Vor allem wird die Jugend gern zu dem Handbuch greifen, um sich schon frühzeitig in militärwissenschaftliche Gedankengänge einzufühlen, ehe für sie die Praxis der Militärzeit beginnt. Aber auch die aktiven und die Offiziere des Beurlaubtenstandes, darüber hinaus Wissenschaftler, Techniker, Männer der Wirtschaft und der Presse sowie der Beamtenschaft werden das Handbuch zum eisernen Bestand ihrer Bücherei rechnen wollen, da es heute keinen Berufszweig gibt, der nicht von Wehrfragen berührt wird. . .“ *DAZ. v. 18. 3. 1936.*

Das Werk wird durch Ergänzungshefte vor dem Veralten geschützt.

Wir liefern Ihnen einen achtseitigen Prospekt, der das vollständige Mitarbeiterverzeichnis und Probeseiten enthält, kostenlos.

Walter de Gruyter & Co. / Berlin W 35

Anzeigenpreise nach Tarif 3. — Verantwortlich für den Anzeigenteil: Kurt Dittrich, Berlin I. v. W. g.